HP ProtectTools
ユーザー ガイド

Bluetooth は、その所有者が所有する商標であり、使用許諾に基づいて Hewlett-Packard Company が使用しています。Java は、米国 Sun Microsystems, Inc.の米国またはその他の国における商標です。Microsoft および Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。SD ロゴは、その所有者の商標です。

本書の内容は、将来予告なしに変更されることがあります。HP 製品およびサービスに関する保証は、当該製品およびサービスに付属の保証規定に明示的に記載されているものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対して責任を負いかねますのでご了承ください。本書に記載されている製品情報は、日本国内で販売されていないものも含まれている場合があります。

初版：2009 年 10 月

製品番号：572661-291

目次

9 File Sanitizer for HP ProtectTools

10 Device Access Manager for HP ProtectTools（一部のモデルのみ）

1 セキュリティの概要

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）ソフトウェアには、コンピューター、ネットワーク、および重要なデータに対する不正アクセスの防止に役立つセキュリティ機能があります。HP ProtectTools Security Manager の管理は、管理者コンソールの機能を通して提供されます。

コンソールを使用すると、ローカルの管理者は以下のタスクを実行できます。

- セキュリティ機能の有効化または無効化
- このコンピューターのユーザーの指紋登録
- スマート カードのセットアップ
- 認証に必要な証明情報の指定
- コンピューターのユーザーの管理
- デバイス固有のパラメーターの調整
- インストールされている HP ProtectTools Security Manager アプリケーションの設定
- HP ProtectTools Security Manager アプリケーションの追加

コンピューターで利用可能なソフトウェア モジュールは、モデルによって異なる可能性があります。

HP ProtectTools ソフトウェア モジュールは、プリインストールまたはプリロードされている場合と、HP の Web サイトからダウンロードできる場合があります。詳しくは、http://www.hp.com/jp/にアクセスしてください。

注記： このガイドの操作手順は、該当する HP ProtectTools ソフトウェア モジュールがすでにインストールされていることを前提に書かれています。

HP ProtectTools の機能

以下の表で、HP ProtectTools モジュールの主な機能を詳しく説明します。

モジュール	主要な機能
Credential Manager for HP ProtectTools	● パスワード マネージャーには、個人のパスワードを保管できます。ユーザーの証明情報を自動的に記憶して適用するシングルサインオン機能を使用してログオン プロセスを効率化します ● また、シングルサインオンは、ユーザー認証に Java™ Card や指紋認証などの異なるセキュリティ テクノロジの組み合わせを要求することによって、さらなる保護機能を提供します ● パスワード記憶域はソフトウェアによる暗号化によって保護されており、さらに Java Card や指紋認証などのセキュリティ デバイス認証を使用することによって保護を強化できます 注記： Credential Manager の機能は、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）のパスワード マネージャー オプションとして提供されています
Drive Encryption for HP ProtectTools（一部のモデルのみ）	● Drive Encryption では、ボリューム全体にわたる完全なハードドライブの暗号化が可能です ● Drive Encryption では、データの暗号化解除やデータへのアクセスにブート前認証が強制されます
Privacy Manager for HP ProtectTools（一部のモデルのみ）	● Privacy Manager は、電子メール、Microsoft® Office ドキュメント、またはインスタント メッセージ（IM）を使用するときに、高度なログオン技術を利用して、通信の発信元、整合性、セキュリティを確認します
File Sanitizer for HP ProtectTools	● File Sanitizer を使用すると、コンピューター上のデジタルのフォルダーやファイル（アプリケーション ファイル、履歴コンテンツや Web 関連コンテンツ、その他の機密データなどの機密情報）を安全にシュレッドしたり、ハードドライブを定期的に「ブリーチ（漂白）」したりすることができます
Device Access Manager for HP ProtectTools（一部のモデルのみ）	● Device Access Manager を使用すると、IT 管理者は、ユーザープロファイルに基づいてデバイスへのアクセスを制御できます ● Device Access Manager は、不正なユーザーが外部のストレージ メディアを使用してデータを削除したり、外部のメディアからシステムにウィルスを侵入させたりできないようにします ● 管理者は、特定の個人またはユーザーのグループに対して、書き込み可能なデバイスへのアクセスを無効にすることができます

主なセキュリティの目的の実現

各 HP ProtectTools モジュールが連携して動作することによって、以下の主なセキュリティの目的を含む、さまざまなセキュリティの問題に対処するためのソリューションを提供できます。

- 盗難からの保護
- 機密データへのアクセス制限
- 内部または外部からの不正なアクセスの防止
- 強力なパスワード ポリシーの作成
- セキュリティを義務付ける規制への対応

盗難からの保護

盗難の例として、空港の検問所での、機密データや顧客情報を含むコンピューターの盗難が挙げられます。盗難からの保護には、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。以下の項目を参照してください。
  - HP ProtectTools Security Manager
  - Drive Encryption for HP ProtectTools

機密データへのアクセス制限

契約検査官がオンサイトで作業していて、機密の財務データの確認のためにコンピューターへのアクセスを許可されているとします。ただし、この検査官がこれらのファイルを印刷したり、CD などの書き込み可能なデバイスに保存できるようにはしたくありません。データへのアクセスを制限するには、以下の機能が役立ちます。

- Device Access Manager for HP ProtectTools を使用すると、IT 管理者は、機密情報を印刷したり、ハードドライブからリムーバブル メディアにコピーしたりできないように、書き込み可能なデバイスへのアクセスを制限することができます。

内部または外部からの不正なアクセスの防止

セキュリティ保護されていない PC への不正なアクセスは、金融サービス、役員、または研究開発チームからのデータなどの社内ネットワーク リソースや、患者記録や個人の財務データなどの個人情報を非常に大きなリスクにさらすことになります。不正なアクセスを防止するには、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。以下の項目を参照してください。
  - パスワード マネージャー
  - Drive Encryption for HP ProtectTools
- パスワード マネージャーは、不正なユーザーがパスワードを入手したり、パスワードで保護されたアプリケーションにアクセスしたりできないようにするために役立ちます。

- Device Access Manager for HP ProtectTools を使用すると、IT 管理者は、機密情報をハードドライブからコピーできないように、書き込み可能なデバイスへのアクセスを制限することができます。
- DriveLock（ドライブロック）は、ハードドライブが取り外されて、セキュリティ保護されていないシステムに取り付けられている場合でもデータにアクセスできないようにするために役立ちます。

強力なパスワード ポリシーの作成

いくつもの Web ベースのアプリケーションやデータベースに対して強力なパスワード ポリシーを使用する必要が生じた場合は、Security Manager を使用することによって、パスワード用の保護されたリポジトリや便利なシングルサインオンを利用できるようになります。

その他のセキュリティ対策

セキュリティの役割の割り当て

コンピューターのセキュリティを（特に、大きな組織で）管理する上では、責任および権限をさまざまな管理者やユーザーに割り当てることが重要な作業の 1 つです。

注記： 小さな組織や個人で使用する場合などは、一人の人がすべての役割を受け持つこともできます。

HP ProtectTools では、セキュリティの責任および権限を以下のように分けられます。

- セキュリティ統括責任者：企業またはネットワークのセキュリティ レベルを定義し、Java Card、指紋認証システム、USB トークンなど、配備するセキュリティ機能を決定します。

  注記： HP ProtectTools の機能の多くは、セキュリティ統括責任者が HP と協力してカスタマイズできます。詳しくは、HP の Web サイト http://www.hp.com/jp/を参照してください。

- IT 管理者：セキュリティ統括責任者によって定義されたセキュリティ機能を適用し、管理します。また、一部の機能を有効または無効にできます。たとえば、セキュリティ統括責任者が Java Card の配備を決定した場合、IT 管理者は Java Card の BIOS セキュリティ モードを有効にすることができます。
- ユーザー：セキュリティ機能を使用します。たとえば、セキュリティ統括責任者および IT 管理者がシステムで Java Card を有効にしている場合、ユーザーは Java Card の PIN を設定し、そのカードを認証に使用できます。

注意： 管理者は、エンド ユーザーの権限の制限や、ユーザー アクセスの制限に関して「ベスト プラクティス（成功事例）」に従うことをおすすめします。

権限のないユーザーには管理者権限を付与しないでください。

HP ProtectTools のパスワードの管理

HP ProtectTools セキュリティ マネージャーの機能のほとんどは、パスワードによってセキュリティ保護されています。以下の表に、よく使用されるパスワード、そのパスワードが設定されるソフトウェア モジュール、およびパスワード機能の一覧を示します。

この表には、IT 管理者のみが設定して使用するパスワードも示されています。その他のすべてのパスワードは、一般のユーザーまたは管理者が設定できます。

HP ProtectTools のパスワード	設定する HP ProtectTools モジュール	機能
Security Manager のログオン パスワード	Security Manager	このパスワードには、以下の 2 つのオプションがあります ● Windows®にログオンした後、Security Manager にアクセスするための Security Manager のログオンとして使用できます ● Windows と Security Manager への同時アクセスを可能にするために使用できます
Security Manager リカバリ ファイルのパスワード	Security Manager、IT 管理者が設定	Security Manager リカバリ ファイルへのアクセスを保護します

HP ProtectTools のパスワード	設定する HP ProtectTools モジュール	機能
Java Card の PIN	Java Card Security	Java Card の内容へのアクセスを保護し、Java Card のユーザーを認証します。電源投入時認証に使用すると、Java Card の PIN の入力によって Computer Setup ユーティリティおよびコンピューターのデータも保護されます Java Card トークンが選択されている場合は、Drive Encryption のユーザーを認証します
Windows のログオン パスワード	Windows の[コントロール パネル]	手動ログオンで使用するか、または Java Card に保存できます

安全なパスワードの作成

パスワードを作成する場合は、まず、プログラムで設定されている仕様に従う必要があります。ただし一般的には、強力なパスワードを作成し、そのパスワードが危険にさらされないようにするために、以下のガイドラインを参考にしてください。

- 文字数が 6 文字、できれば 8 文字を超えるパスワードを使用します。
- パスワード全体にわたって大文字と小文字を混在させます。
- 可能な場合は、常に半角アルファベットと半角数字を混在させ、さらに特殊文字と句読点を含めます。
- パスワード中の文字の代わりに特殊文字または数字を使用します。たとえば、アルファベットの I または L の代わりに数字の 1 を使用します。
- 2 つ以上の言語から取った単語を組み合わせます。
- 単語またはフレーズを数字や特殊文字で分けます。たとえば、「Mary2-2Cat45」とします。
- 辞書に載っているような用語は使用しないでください。
- 名前やその他の個人情報（たとえば、誕生日、ペットの名前、母親の旧姓など）は、たとえ綴りを逆にしたとしても、パスワードには使用しないでください。
- パスワードは定期的に変更してください。いくつかの文字や数字をその次の値に変更するのみでも構いません。
- パスワードをメモした場合は、コンピューターのすぐ近くの、人目につきやすい場所に保管しないでください。
- パスワードを、電子メールなどのコンピューター上のファイルに保存しないでください。
- アカウントを共有したり、パスワードを誰かに教えたりしないでください。

HP ProtectTools 証明情報のバックアップおよび復元

Drive Encryption for HP ProtectTools を使用して、HP ProtectTools 証明情報を選択したりバックアップしたりできます。

2 お使いになる前に

注記： HP ProtectTools の管理には管理者権限が必要です。

HP ProtectTools セットアップ ウィザードでは、Security Manager で最もよく使用する機能を設定できます。また、HP ProtectTools 管理者コンソールを通して使用できる豊富な追加機能があります。ウィザードにあるものと同じ設定や、追加のセキュリティ機能は、Windows の[スタート]メニューからアクセスできるコンソールを使用して設定できます。これらの設定は、コンピューターおよび、そのコンピューターを共有しているすべてのユーザーに適用されます。

1. [ようこそ]ページで、オプションの 1 つを選択して、ウィザードの以降の表示を無効にできます。
2. コンピューターの設定後 1 週間が経過したとき、または管理者権限を持つユーザーが最初に指紋認証システムに指を滑らせたときに、HP ProtectTools セットアップ ウィザードが自動的に起動し、このプログラムを設定するための基本的な手順を実行します。コンピューターのセットアップに関する動画のチュートリアルが自動的に開始されます。
3. セットアップが完了するまで、画面の説明に沿って操作します。

ウィザードを完了しなかった場合は、さらに 2 回自動的に起動されます。その後、セットアップが完了するまで、タスクバー通知領域の近くに表示される通知用バルーンからウィザードにアクセスできます（上記の手順 2 で説明した方法で無効にしている場合を除きます）。

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）アプリケーションを使用するには、[スタート]メニューから HP ProtectTools Security Manager を起動するか、またはタスクバーの右端の通知領域にある[HP ProtectTools Security Manager]アイコンを右クリックします。HP ProtectTools 管理者コンソールおよびそのアプリケーションは、このコンピューターを共有しているすべてのユーザーが使用できます。

HP ProtectTools 管理者コンソールを開く

システム ポリシーの設定やソフトウェアの設定などの管理タスクの場合は、以下の操作を行ってコンソールを開きます。

▲ **[スタート]→[すべてのプログラム]→[HP]→[HP ProtectTools 管理者コンソール]**の順にクリックします。

または

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）の左側の枠内で、**[管理]**をクリックします。

指紋の登録や HP ProtectTools Security Manager の使用などのユーザー タスクの場合は、以下の操作を行ってコンソールを開きます。

▲ **[スタート]→[すべてのプログラム]→[HP]→[HP ProtectTools Security Manager]**の順にクリックします。

または

タスクバーの右端の通知領域にある**[HP ProtectTools Security Manager]**アイコンをダブルクリックします。

セキュリティ機能の有効化

セットアップ ウィザードではユーザー情報の認証を行うよう求められます。

1. [ようこそ]画面の内容を確認して、**[次へ]**をクリックします。
2. Windows パスワードを入力するか（指紋がまだ登録されていない場合）、または指紋認証システムを使用して指紋をスキャンすることによって、ユーザー情報を認証します。**[次へ]**をクリックします。

   Windows パスワードが空白の場合は、Windows パスワードを作成するよう求められます。お使いの Windows アカウントが第三者から不正にアクセスされないようにするために、また HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）の機能を使用するためには、Windows パスワードが必要となります。

セットアップ ウィザードでは、コンピューターのすべてのユーザーに適用されるセキュリティ機能を有効にするプロセスを実行します。

- Windows へのログオンの保護機能を使用すると、アクセスのために特定の証明情報を使用するよう求めることで、Windows アカウントを保護できます。
- ドライブの暗号化機能を使用すると、ハードドライブを暗号化して、適切な権限のないユーザーが情報を読み取れないようにすることによってデータを保護できます。
- ブート前セキュリティ機能を使用すると、Windows の起動前に、不正なユーザーによるアクセスを禁止することによってコンピューターを保護できます。

セキュリティ機能を有効にするには、対応するチェック ボックスにチェックを入れます。選択する機能が多いほど、コンピューターのセキュリティは高くなります。

注記： BIOS によってサポートされていない場合は、[ブート前セキュリティ]を使用できません。

指紋の登録

[指紋]を選択し、コンピューターに指紋認証システムが内蔵または接続されている場合は、指紋の設定または「登録」のプロセスを実行できます。

1. 両手の輪郭が表示されます。すでに登録されている指は緑色で強調表示されます。輪郭で示されている指をクリックします。

   注記： 以前に登録された指紋を削除するには、対応する指をクリックします。

2. 登録する指を選択すると、正常に登録されるまでその指紋をスキャンするよう求められます。登録された指は、輪郭が付いて緑色で強調表示されます。

3. 少なくとも 2 本の指を登録する必要があります。人差し指または中指をおすすめします。別の指を登録するには、手順 1 から 3 を繰り返します。

4. **[次へ]**をクリックします。

注記： [ここから開始]のプロセスで指紋を登録している場合は、**[次へ]**をクリックするまで指紋の情報が保存されません。コンピューターをしばらくアイドル状態にしていた場合や、ダッシュボードを閉じた場合は、それ以前に行った変更が保存されません。

スマート カードのセットアップ

[スマート カード]を選択し、コンピューターにスマート カード リーダーが内蔵または接続されている場合は、HP ProtectTools セットアップ ウィザードからスマート カードの PIN（個人識別番号）を設定するよう求めるメッセージが表示されます。

スマート カードの PIN をセットアップするには、以下の操作を行います。

1. [スマート カードのセットアップ]ページで、PIN を入力して確認します。

   PIN を変更することもできます。古い PIN を入力してから、新しい PIN を選択します。

2. 続行するには、**[次へ]**をクリックします。

管理者コンソールの使用

HP ProtectTools 管理者コンソールは、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）の機能およびアプリケーションを管理するための中心となる場所です。

このコンソールは、以下のコンポーネントで構成されています。

- **[ツール]**：コンピューターのセキュリティを設定するための以下のカテゴリを表示します。
  - **[ホーム]**：実行するセキュリティ タスクを選択できます。
  - **[システム]**：ユーザーやデバイスのセキュリティ機能および認証を設定できます。
  - **[アプリケーション]**：HP ProtectTools Security Manager および HP ProtectTools Security Manager アプリケーションの一般的な設定を表示します。
  - **[データ]**：データを保護する HP ProtectTools Security Manager アプリケーションへのリンクの展開メニューを提供します。
- **[管理ツール]**：追加のツールに関する情報を提供します。下のパネルに、以下の選択肢が表示されます。
  - **[HP ProtectTools セットアップ ウィザード]**：HP ProtectTools Security Manager を設定できます。
  - **[ヘルプ]**：HP ProtectTools Security Manager およびプリインストールされているアプリケーションに関する情報を提供するヘルプ ファイルを表示します。追加できるアプリケーションのヘルプは、これらのアプリケーション内で提供されます。
  - **[バージョン情報]**：バージョン番号や著作権情報などの、HP ProtectTools Security Manager に関する情報を表示します。
- **メイン領域**：アプリケーション固有の画面を表示します。

HP ProtectTools 管理者コンソールを開くには、**[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools 管理者コンソール]**の順にクリックします。

3 システムの設定

[システム]グループには、HP ProtectTools 管理者コンソールの画面の左側にある[ツール]メニュー パネルからアクセスします。このグループ内のアプリケーションを使用して、コンピューター、ユーザー、およびデバイスのポリシーや設定を管理できます。

[システム]グループには、以下のアプリケーションが含まれています。

- **[セキュリティ]**：このコンピューターに対する、ユーザーの対話操作の方法を管理する機能、認証、および設定を管理します。
- **[ユーザー]**：このコンピューターのユーザーを設定、管理、および登録します。
- **[デバイス]**：コンピューターに内蔵または接続されているセキュリティ デバイスの設定を管理します。

コンピューターでの認証の設定

認証アプリケーション内では、このコンピューターに実装するセキュリティ機能を選択したり、コンピューターへのアクセスを管理するポリシーを設定したり、追加の詳細設定を設定したりできます。Windows にログオンするとき、またはユーザー セッション中に Web サイトやプログラムにログインする場合に各クラスのユーザーを認証するために必要な証明情報を指定できます。

コンピューターでの認証を設定するには、以下の操作を行います。

1. [セキュリティ]パネル メニューで、**[認証]**をクリックします。
2. ログオン認証を設定するには、**[ログオン ポリシー]**タブをクリックし、変更を行ってから**[適用]**をクリックします。
3. セッション認証を設定するには、**[セッション ポリシー]**タブをクリックし、変更を行ってから**[適用]**をクリックします。

ログオン ポリシー

Windows にログオンするときにユーザーを認証するために必要な証明情報を管理するポリシーを定義するには、以下の操作を行います。

1. [ツール]メニューで**[セキュリティ]**をクリックし、**[認証]**をクリックします。
2. **[ログオン ポリシー]**タブでユーザーのカテゴリをクリックします。
3. 選択したユーザーのカテゴリに必要な認証証明情報を指定します。少なくとも 1 つの証明情報を指定する必要があります。
4. ユーザーを認証するために、指定した証明情報のどれか（1 つのみ）が必要なのか、または指定した証明情報のすべてが必要なのかを選択します。他のユーザーが、コンピューターにアクセスできなくなるようにすることもできます。
5. **[適用]**をクリックします。

セッション ポリシー

Windows セッション中に HP ProtectTools アプリケーションにアクセスするために必要な証明情報を管理するポリシーを定義するには、以下の操作を行います。

1. [ツール]メニューで**[セキュリティ]**をクリックし、**[認証]**をクリックします。
2. **[セッション ポリシー]**タブでユーザーのカテゴリをクリックします。
3. 選択したユーザーのカテゴリに必要な認証証明情報を指定します。
4. ユーザーを認証するために、指定した証明情報のどれか（1 つのみ）が必要なのか、または指定した証明情報のすべてが必要なのかを選択します。HP ProtectTools ソフトウェアへのアクセスに認証を求めないようにすることもできます。
5. **[適用]**をクリックします。

設定

以下の 1 つ以上のセキュリティ設定を許可できます。

- **[ワン ステップ ログオンを許可する]**：BIOS または暗号化されたディスクのレベルで認証が実行された場合は、このコンピューターのユーザーが Windows のログオンを省略できるようにします。
- **[Windows のログオンに HP SpareKey 認証を許可する]**：HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）によって他の何らかの認証ポリシーが求められる場合でも、このコンピューターのユーザーが HP SpareKey 機能を使用して Windows にログオンできるようにします。

設定を編集するには、以下の操作を行います。

1. 特定の設定をクリックして有効または無効にします。
2. **[適用]**をクリックして、行った変更を保存します。

ユーザーの管理

ユーザー アプリケーション内で、このコンピューターの HP ProtectTools ユーザーを監視したり管理したりできます。

すべての HP ProtectTools ユーザーが一覧表示され、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）を使用して設定されたポリシーに対して検証されます。一覧表示および検証は、これらのユーザーが各ポリシーを満たすことができる適切な証明情報を登録しているかどうかに関係なく行われます。

ユーザーを追加するには、**[追加]**をクリックします。

ユーザーを削除するには、そのユーザーをクリックしてから**[削除]**をクリックします。

ユーザーの指紋を登録するか、または追加の証明情報を設定するには、そのユーザーをクリックしてから、**[登録]**をクリックします。

特定のユーザーのポリシーを表示するには、そのユーザーを選択してから**[ポリシーの表示]**をクリックします。

デバイス設定の指定

デバイス アプリケーション内で、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）によって認識される内蔵または接続されている任意のセキュリティ デバイスで使用できる設定を指定できます。

指紋

[指紋]ページには、[登録]、[感度]、[詳細]の 3 つのタブがあります。

登録

ユーザーが登録できる指紋の最小数と最大数を選択できます。

また、指紋認証システムからすべてのデータをクリアすることもできます。

⚠ **警告！** 管理者を含む、すべてのユーザーの指紋データが消去されます。ログオン ポリシーで指紋のみを求めるようにしている場合は、すべてのユーザーがコンピューターにログオンできなくなることがあります。

感度

指紋がスキャンされるときに指紋認証システムで使用される感度を調整するには、スライダーを移動します。

指紋が常に認識されない場合は、より低い感度に設定することが必要な可能性があります。この設定を高くすると指紋スキャンの変化に対する感度が向上するため、誤って受け入れられる可能性が減ります。[中-高]に設定すると、セキュリティおよび利便性の適切な組み合わせが得られます。

詳細

コンピューターがバッテリ電源で動作しているときは、電力を節約するように指紋認証システムを設定できます。

スマート カード

スマート カードが取り外されたときは、自動的にロックするようにコンピューターを設定できます。ただし、コンピューターがロックするのは、そのスマート カードが Windows へのログオン時の認証証明情報として使用されていた場合のみです。Windows へのログオンに使用されていなかったスマート カードを取り外しても、コンピューターはロックされません。

▲ スマート カードが取り外されたときのコンピューターのロックを有効または無効にするには、チェック ボックスにチェックを入れます。

4 アプリケーションの設定

[アプリケーション]グループには、HP ProtectTools 管理者コンソールの左側にある[セキュリティ アプリケーション]メニュー パネルからアクセスします。[設定]を使用して、現在インストールされている HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）アプリケーションの動作をカスタマイズできます。

アプリケーションの設定を編集するには、以下の操作を行います。

1. [ツール]メニューで、**[アプリケーション]**グループから**[設定]**をクリックします。
2. 特定の設定をクリックして有効または無効にします。
3. **[適用]**をクリックして、行った変更を保存します。

[全般]タブ

[全般]タブでは、以下の設定を使用できます。

- **[管理者用のセットアップ ウィザードを自動的に起動しない]**：ログオン時にウィザードが自動的に開かないようにするには、このオプションを選択します。
- **[ユーザー用の使用開始準備ウィザードを自動的に起動しない]**：ログオン時にユーザーの設定が自動的に開かないようにするには、このオプションを選択します。

[アプリケーション]タブ

ここに表示される設定は、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）に新しいアプリケーションが追加されると変更される可能性があります。初期設定で表示される最小限の設定は、以下のとおりです。

- **[Security Manager]**：コンピューターのすべてのユーザーに対して HP ProtectTools Security Manager アプリケーションを有効にします。
- **[[他を検出]ボタンを有効にする]**：このコンピューターのすべてのユーザーが**[[+]他を検出]**ボタンをクリックすることによって HP ProtectTools Security Manager にアプリケーションを追加できるようにします。

すべてのアプリケーションを工場出荷時の設定に戻すには、**[初期設定に設定]**ボタンをクリックします。

5　管理ツールの追加

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）では、新しい管理ツールを追加するために、追加のアプリケーションを使用できます。このコンピューターの管理者は、設定アプリケーションを使用してこの機能を無効にできます。

管理ツールを追加するには、**[[+]管理ツール]**をクリックします。

DigitalPersona の Web サイトにアクセスして、新しいアプリケーションを確認するか、自動アップデートのスケジュールを設定できます。

6 HP ProtectTools Security Manager

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）を使用すると、お使いのコンピューターのセキュリティを大幅に強化できます。

プリロードされている HP ProtectTools Security Manager の各アプリケーション、および Web からいつでもダウンロードできる追加アプリケーションを使用して、以下のタスクを実行できます。

- ログオンおよびパスワードを管理する
- Windows オペレーティング システムのパスワードを簡単に変更する
- プログラムのオプションを設定する
- 指紋を利用してセキュリティと利便性を強化する
- 認証用のスマート カードをセットアップする
- プログラムのバックアップおよび復元を実行する
- アプリケーションをさらに追加する

セットアップ手順

お使いになる前に

セットアップが完了するまでは、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）を起動すると、HP ProtectTools セットアップ ウィザードが初期設定のページとして自動的に表示されます。

HP ProtectTools Security Manager のセットアップを行うには、以下の操作を行います。

注記： 指紋認証システムとスマート カードのどちらも利用できない場合は、手順 1、5、および 6 のみを実行してください。

1. [ようこそ]ページで**[次へ]**をクリックします。
2. このコンピューターで使用できる認証方法が、次のページに一覧表示されます。作業を続けるには**[次へ]**をクリックします。
3. [ユーザー情報の認証]ページで Windows パスワードを入力して、**[次へ]**をクリックします。
4. お使いのコンピューターの構成に応じて、以下のどちらかまたは両方のトピックを参照してください。
   - 指紋認証システムが利用できる場合は、24 ページの 「指紋の登録」を参照してください。
   - スマート カードが利用できる場合は、25 ページの 「スマート カードのセットアップ」を参照してください。
5. 指紋認証システムとスマート カードのどちらも利用できない場合は、Windows パスワードを入力するよう求められます。以降は、認証を求められるたびにこのパスワードを使用する必要があります。
6. ウィザードの最後のページで、**[完了]**をクリックします。

   [HP ProtectTools Security Manager]ダッシュボードが表示されます。

証明情報の登録

[個人 ID]ページを使用して、各種の認証方法、または証明情報を登録できます。登録が完了した後、それらの方法を使用して HP ProtectTools Security Manager にログオンできます。

指紋の登録

コンピューターに指紋認証システムが内蔵または接続されている場合は、HP ProtectTools セットアップ ウィザードの説明に沿って指紋を設定（指紋認証システムの用語としては「登録」）します。

1. [ようこそ]画面の内容を確認して、**[次へ]**をクリックします。
2. Windows パスワードを入力するか（指紋がまだ登録されていない場合）、または指紋認証システムを使用して指紋をスキャンすることによって、ユーザー情報を認証します。**[次へ]**をクリックします。

   Windows パスワードが空白の場合は、Windows パスワードを作成するよう求められます。お使いの Windows アカウントが第三者から不正にアクセスされないようにするために、また HP ProtectTools Security Manager の機能を使用するためには、Windows パスワードが必要となります。

3. 両手の輪郭が表示されます。すでに登録されている指は緑色で強調表示されます。輪郭で示されている指をクリックします。

   注記： 以前に登録された指紋を削除するには、対応する指紋をクリックします。

4. 登録する指を選択すると、正常に登録されるまでその指紋をスキャンするよう求められます。登録された指は、輪郭が付いて緑色で強調表示されます。

5. 少なくとも 2 本の指を登録する必要があります。人差し指または中指をおすすめします。別の指を登録するには、手順 3 および 4 を繰り返します。

6. **[次へ]**をクリックします。

注記： [ここから開始]のプロセスで指紋を登録している場合は、手順 6 の**[次へ]**をクリックするまで指紋の情報が保存されません。コンピューターをしばらくアイドル状態にしていた場合や、ダッシュボードを閉じた場合は、それ以前に行った変更が保存されません。

Windows パスワードの変更

HP ProtectTools Security Manager を使用すると、Windows の[コントロール パネル]を使用するよりも、すばやく簡単に Windows パスワードを変更できます。

Windows パスワードを変更するには、以下の操作を行います。

1. [HP ProtectTools Security Manager]ダッシュボードで、**[個人 ID]**→**[証明書]**→**[パスワード]**の順にクリックします。

2. **[現在の Windows パスワード]**テキスト ボックスに、現在のパスワードを入力します。

3. **[新しい Windows パスワード]**テキスト ボックスに新しいパスワードを入力し、**[新しいパスワードの確認]**テキスト ボックスにそのパスワードを再度入力します。

4. **[変更]**をクリックすると、現在のパスワードが、入力した新しいパスワードにすぐに変更されます。

スマート カードのセットアップ

コンピューターにスマート カード リーダーが内蔵または接続されている場合は、HP ProtectTools Security Manager から、スマート カードの PIN（個人識別番号）をセットアップするよう求めるメッセージが表示されます。

- スマート カードの PIN をセットアップするには、[スマート カードのセットアップ]ページで、PIN を入力して確認します。

- PIN を変更するには、最初に現在の PIN を入力してから、新しい PIN を選択します。

[HP ProtectTools Security Manager]ダッシュボードの使用

[HP ProtectTools Security Manager]ダッシュボードは、HP ProtectTools Security Manager の機能、アプリケーション、および設定に簡単にアクセスするための中心となる場所です。

ダッシュボードは以下のコンポーネントで構成されています。

- **[ID カード]**：ログオン中のユーザー アカウントを識別する、Windows ユーザー名および選択済みの画像を表示します。
- **[セキュリティ アプリケーション]**：以下のカテゴリのセキュリティを設定できる、リンクの展開メニューを提供します。
  - **個人 ID**
  - **個人のデータ**
  - **個人のコンピューター**
- **[他を検索]**：ID、データ、および通信のセキュリティを強化するための追加アプリケーションを検索できるページが表示されます。
- **[メイン領域]**：アプリケーション固有の画面を表示します。
- **[管理]**：[HP ProtectTools 管理者コンソール]が表示されます。
- **[ヘルプ]**ボタン：現在表示されている画面についての情報を表示します。
- **[詳細設定]**：次のオプションにアクセスできます。
  - **[オプション]**：HP ProtectTools Security Manager の個人設定を実行できます。
  - **[バックアップおよび復元]**：データをバックアップまたは復元できます。
  - **[バージョン情報]**：HP ProtectTools Security Manager のバージョン情報を表示します。

[HP ProtectTools Security Manager]ダッシュボードを開くには、**[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools Security Manager]**の順にクリックします。

HP ProtectTools Security Manager を開く

以下のどれかの方法で HP ProtectTools Security Manager を開きます。

- **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools Security Manager]**の順にクリックします。
- タスクバーの右端の通知領域にある**[HP ProtectTools]**アイコンをダブルクリックします。
- **[HP ProtectTools]**アイコンを右クリックして、**[HP ProtectTools Security Manager を開く]**をクリックします。
- Windows サイドバーで HP ProtectTools Security Manager の**[ID カード]**ガジェットをクリックします。
- ctrl ＋ alt ＋ h ホットキーを使用して、HP ProtectTools Security Manager の[クイック リンク]メニューを開きます。

一般的なタスク

このグループに含まれるアプリケーションによって、ユーザーのデジタル ID をさまざまな面から管理することができます。

- **[HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）]**：クイック リンクを作成および管理します。クイック リンクを使用すると、Windows パスワード、指紋、またはスマート カードによる認証を行うことで、Web サイトおよびプログラムを起動し、ログオンすることができます。
- **[証明書]**：Windows パスワードの変更、指紋の登録、またはスマート カードのセットアップを簡単に実行できるようにします。

アプリケーションをさらに追加するには、ダッシュボードの左下隅にある**[[＋]他を検出]**ボタンをクリックします。このボタンは、管理者によって無効にされている場合があります。

パスワード マネージャー

パスワード マネージャーを使用すると、Windows、Web サイト、およびアプリケーションへのログオンがより簡単かつ安全になります。書き留めておいたり覚えておいたりする必要がない強固なパスワードをパスワード マネージャーで作成できるため、指紋、スマート カード、または Windows パスワードを使用してすばやく簡単にログオンできるようになります。

パスワード マネージャーには以下のオプションがあります。

- [管理]タブでログオンを追加、編集、または削除する。
- クイック リンクを使用して初期設定のブラウザーを起動し、セットアップ済みの Web サイトまたはプログラムにログオンする。
- ドラッグ アンド ドロップ操作でクイック リンクをカテゴリ別に整理する。
- セキュリティ上のリスクがあるパスワードをすぐに見つけ出し、複雑で強固なパスワードを自動生成して新しいサイトで利用できるようにする。

Web ページまたはプログラムのログオン画面がフォーカスされているときに表示される[パスワード マネージャー]アイコンからも、パスワード マネージャーの多くの機能を利用できます。このアイコンをクリックしてコンテキスト メニューを表示すると、以下のオプションを選択できます。

ログオンが作成されていない Web ページまたはプログラムの場合

以下のオプションがコンテキスト メニューに表示されます。

- **[[任意のドメイン]をパスワード マネージャーに追加]**：表示中のログオン画面用にログオンを追加できます。
- **[パスワード マネージャーを起動]**：パスワード マネージャーを起動します。
- **[アイコンの設定]**：[パスワード マネージャー]アイコンを表示する条件を指定できます。
- **[ヘルプ]**：パスワード マネージャー ソフトウェアのヘルプを表示します。

ログオンが作成されている Web ページまたはプログラムの場合

以下のオプションがコンテキスト メニューに表示されます。

- **[ログオン データの入力]**：ログオン データをログオン用フィールドに入力してページを送信します（ログオンを作成または最後に編集したときに送信を指定していた場合）。
- **[ログオンの編集]**：表示中の Web サイト用のログオン データを編集できます。
- **[新規アカウントの追加]**：アカウントをログオンに追加できます。
- **[パスワード マネージャーを起動]**：パスワード マネージャー アプリケーションを起動します。
- **[ヘルプ]**：パスワード マネージャー ソフトウェアのヘルプを表示します。

注記： HP ProtectTools Security Manager は、証明情報を確認するときに、複数の証明情報が求められるようにコンピューターの管理者によってセットアップされていることがあります。

ログオンの追加

Web サイトまたはプログラム用のログオンは、ログオン情報を 1 回入力すれば、簡単に追加できます。以降は、パスワード マネージャーによって情報が自動的に入力されるようになります。これらのログオンは、その Web サイトまたはプログラムを表示すると使用できるようになります。また、**[ログオン]**メニューからログオンをクリックし、パスワード マネージャーでその Web サイトまたはプログラムを表示させてログオンすることもできます。

ログオンを追加するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. **[パスワード マネージャー]**アイコンの矢印をクリックし、ログオン画面の種類（Web サイト用またはプログラム用）に応じて以下のどちらかをクリックします。
   - Web サイトの場合は、**[[任意のドメイン]をパスワード マネージャーに追加]**をクリックします。
   - プログラムの場合は、**[このログオン画面をパスワード マネージャーに追加]**をクリックします。
3. ログオン データを入力します。画面のログオン用フィールドおよびダイアログ ボックスの対応するフィールドが、オレンジ色の太い枠線で識別されます。**[パスワード マネージャーの管理]**タブから**[ログオンの追加]**をクリックして、このダイアログ ボックスを表示させることもできます。ctrl ＋ alt ＋ h ホットキーを使用して指紋のスキャンやスマート カードの挿入を実行できるオプションなど、コンピューターに接続されているセキュリティ デバイスに依存するオプションもあります。
   - あらかじめフォーマットが用意された選択肢の 1 つを使用してログオン用フィールドに入力するには、フィールドの右側にある矢印をクリックします。
   - 画面上の他のフィールドをログオンに追加するには、**[他のフィールドの選択]**をクリックします。
   - ログオン用フィールドの入力後に送信を実行しない場合は、**[ログオン データの送信]**チェック ボックスのチェックを外します。
   - このログオン用のパスワードを表示するには、**[パスワードの表示]**をクリックします。
4. **[OK]**をクリックします。

[パスワード マネージャー]アイコンのプラス記号（＋）が消え、ログオンが作成されたことが示されます。

この Web サイトまたはプログラムにアクセスすると、その度に[パスワード マネージャー]アイコンが表示され、登録済みの証明情報を使用してログオンできることが示されます。

ログオンの編集

ログオンを編集するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. ログオン情報を編集できるダイアログ ボックスを表示するには、**[パスワード マネージャー]**アイコンの矢印→**[ログオンの編集]**の順にクリックします。画面のログオン用フィールドおよびダイアログ ボックスの対応するフィールドが、オレンジ色の太い枠線で識別されます。

   [パスワード マネージャーの管理]タブから**[目的のログオンの編集]**をクリックして、このダイアログ ボックスを表示させることもできます。
3. ログオン情報を編集します。
   - あらかじめフォーマットが用意された選択肢の 1 つを使用してログオン用フィールドに入力するには、フィールドの右側にある矢印をクリックします。
   - 画面上の他のフィールドをログオンに追加するには、**[他のフィールドの選択]**をクリックします。
   - ログオン用フィールドの入力後に送信を実行しない場合は、**[ログオン データの送信]**チェック ボックスのチェックを外します。
   - このログオン用のパスワードを表示するには、**[パスワードの表示]**をクリックします。
4. **[OK]**をクリックします。

ログオン メニューの使用

パスワード マネージャーでは、ログオンを作成した Web サイトおよびプログラムをすばやく簡単に起動できます。**[ログオン]**メニューまたは**[パスワード マネージャー]**の**[管理]**タブからプログラムまたは Web サイトをダブルクリックし、ログオン画面を表示して、ログオン データを入力します。

作成したログオンは、パスワード マネージャーの[ログオン]メニューに自動的に追加されます。

[ログオン]メニューを表示するには、以下の操作を行います。

1. パスワード マネージャーのホットキーを押します。工場出荷時の設定では ctrl ＋ alt ＋ h になっています。ホットキーを変更するには、**[パスワード マネージャー]**→**[設定]**の順にクリックします。
2. （指紋認証システムが内蔵または接続されたコンピューターで）指紋をスキャンします。

ログオンをカテゴリ別に整理

ログオンを整理するには、カテゴリを使用します。これを行うには、1 つ以上のカテゴリを作成します。その後、ログオンを目的のカテゴリにドラッグ アンド ドロップします。

カテゴリを追加するには、以下の操作を行います。

1. [HP ProtectTools Security Manager]ダッシュボードで、**[パスワード マネージャー]**をクリックします。
2. **[管理]**タブ→**[カテゴリの追加]**の順にクリックします。
3. カテゴリの名前を入力します。
4. **[OK]**をクリックします。

ログオンをカテゴリに追加するには、以下の操作を行います。

1. マウス ポインターを目的のログオンの上に置きます。
2. マウスの左ボタンを押したままにします。
3. ログオンをカテゴリの一覧にドラッグします。マウスをカテゴリの上に置くと、そのカテゴリが強調表示されます。
4. 目的のカテゴリが強調表示されたら、マウス ボタンを放します。

ログオンは、選択したカテゴリに移動されるのではなく、コピーされるのみです。そのため、同じログオンを複数のカテゴリに追加できます。**[すべて]**をクリックするとすべてのログオンを表示できます。

ログオンの管理

パスワード マネージャーを使用すると、ユーザー名、パスワード、および複数のログオン アカウントのログオン情報を、中心となる 1 つの場所から簡単に管理できます。

ログオンは[管理]タブに一覧表示されます。同じ Web サイトに対して複数のログオンが作成されている場合、各ログオンはその Web サイト名の下に一覧表示され、ログオン一覧の中でインデント表示されます。

ログオンを管理するには、以下の操作を行います。

[HP ProtectTools Security Manager]ダッシュボードで、**[パスワード マネージャー]**→**[管理]**タブの順にクリックします。

- **ログオンの追加**：**[ログオンの追加]**をクリックし、画面の説明に沿って操作します。
- **ログオンの編集**：[ログオン]→**[編集]**の順にクリックし、ログオン データを変更します。
- **ログオンの削除**：[ログオン]→**[削除]**の順にクリックします。

Web サイトまたはプログラムに他のログオンを追加するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. **[パスワード マネージャー]**アイコンをクリックして、ショートカット メニューを表示します。
3. **[他のログオンの追加]**をクリックし、画面の説明に沿って操作します。

パスワード強度の評価

証明情報を保護するには、Web サイトおよびプログラムに強固なパスワードを使用することが重要です。

パスワード マネージャーでは、Web サイトおよびプログラムへのログオンに使用されている各パスワードの強度を自動的にすばやく分析することで、セキュリティを監視および強化できます。

[パスワード マネージャー]アイコンの設定

パスワード マネージャーは、Web サイトおよびプログラムのログオン画面を識別します。ログオンが作成されていないログオン画面が検出されると、パスワード マネージャーによってプラス記号（＋）の付いた[パスワード マネージャー]アイコンが表示され、そのログオン画面用のログオンを追加するよう求められます。

ログオン可能なサイトでの**[パスワード マネージャー]**の動作方法をカスタマイズするには、アイコンの矢印→**[アイコンの設定]**の順にクリックします。

- **[ログオン画面へのログオンの追加を要求]**：ログオンがまだ設定されていないログオン画面が表示されたときに、パスワード マネージャーによってログオンの追加が求められるようにするには、このオプションをクリックします。
- **[この画面を除外する]**：このログオン画面へのログオンの追加をパスワード マネージャーによって二度と求められないようにするには、このチェックボックスにチェックを入れます。

パスワード マネージャーの詳細設定にアクセスするには、[HP ProtectTools Security Manager]ダッシュボードで**[パスワード マネージャー]**→**[設定]**の順にクリックします。

設定

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）では、以下の個人設定を指定できます。

1. **[ログオン画面へのログオンの追加を要求]**：Web サイトまたはプログラムのログオン画面が検出されるたびに[パスワード マネージャー]アイコンをプラス記号（＋）付きで表示し、この画面のログオンを追加してパスワードを保管できることを示します。この機能を無効にするには、**[アイコンの設定]**ダイアログ ボックスで**[ログオン画面へのログオンの追加を要求]**の横にあるチェック ボックスのチェックを外します。
2. **[ctrl ＋ alt ＋ h でパスワード マネージャーを開く]**：パスワード マネージャーの[クイック リンク]メニューを開くための初期設定のホットキーは、ctrl ＋ alt ＋ h です。このホットキーを変更するには、このオプションをクリックして新しいキーの組み合わせを入力します。ctrl、alt、shift、および任意の英数字キーを組み合わせることができます。
3. **[適用]**をクリックして変更を保存します。

証明情報

HP ProtectTools Security Manager の証明情報を使用して、ユーザーが本人であることを確認します。このコンピューターのローカル管理者は、Windows アカウント、Web サイト、またはプログラムにログオンするユーザーが証明情報の確認に使用できる証明情報の種類を設定できます。

使用できる証明情報は、このコンピューターに内蔵または接続されているセキュリティ デバイスの種類によって異なります。サポートされる証明情報は、**[個人 ID、証明書]**グループに登録されます。

使用できる証明情報、要件、および現在の状態が一覧表示されるほか、以下のどれかまたはすべての情報が含まれます。

- 指紋
- パスワード
- スマート カード

証明情報を登録または変更するには、その証明情報のリンクをクリックし、画面の説明に沿って操作します。

個人用 ID カード

ID カードは、ユーザーの名前およびユーザーが選択した写真を表示して、Windows アカウントの所有者を一意に識別します。ID カードは、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）の各ページの左上隅に、また Windows サイドバー ガジェットとして、目立つような形で表示されます。

HP ProtectTools Security Manager にすばやくアクセスするにはさまざまな方法がありますが、Windows サイトバーの ID カードをクリックするのがその方法の 1 つです。

画像および名前の表示方法は変更できます。初期設定では、Windows のセットアップ中に選択した完全な Windows ユーザー名および画像が表示されます。

表示名を変更するには、以下の操作を行います。

1. [HP ProtectTools Security Manager]ダッシュボードの左上隅で、**[ID カード]**をクリックします。
2. Windows のアカウント用に入力した名前を表示しているボックスをクリックします。このアカウントの Windows ユーザー名がシステムによって表示されます。
3. この名前を変更するには、新しい名前を入力して、**[保存]**ボタンをクリックします。

表示画像を変更するには、以下の操作を行います。

1. [HP ProtectTools Security Manager]ダッシュボードの左上隅で、**[個人 ID]**→**[ID カード]**の順にクリックします。
2. **[画像の選択]**ボタン→画像→**[保存]**ボタンの順にクリックします。

オプションの設定

HP ProtectTools Security Manager では、個人設定を指定できます。[HP ProtectTools Security Manager]ダッシュボードで、**[詳細設定]**→**[オプション]**の順にクリックします。使用可能な設定が、[全般]と[指紋]の 2 つのタブに表示されます。

全般

[全般]タブでは、以下の設定を使用できます。

[外観：アイコンをタスク バーに表示する]

タスク バーへのアイコンの表示を有効にするには、このチェック ボックスにチェックを入れます。

タスク バーへのアイコンの表示を無効にするには、このチェック ボックスのチェックを外します。

指紋

[指紋]タブでは、以下の設定を使用できます。

[クイック アクション]：クイック アクションを使用すると、割り当てたキーを指紋のスキャン中に押したままにしたときに実行される HP ProtectTools Security Manager タスクを選択できます。

クイック アクションを一覧のどれかのキーに割り当てるには、以下の操作を行います。

- **[（キー）＋指紋]**オプションをクリックして、使用可能なタスクをメニューから 1 つ選択します。

[指紋スキャンのフィードバック]：指紋認証システムが使用できる場合にのみ表示されます。この設定を使用すると、指紋をスキャンしたときに返されるフィードバックを調整できます。

- **[サウンド フィードバックを有効にする]**：指紋がスキャンされたときに、HP ProtectTools Security Manager によってサウンドのフィードバックが返されます。プログラム イベントごとに異なるサウンドが再生されます。Windows の[コントロール パネル]の[サウンド]タブでイベントに新しいサウンドを割り当てるか、このオプションを選択解除してサウンドのフィードバックを無効にすることができます。
- **[スキャン品質のフィードバックを表示]**：初期設定では、指紋スキャンの質が認証の実行に十分でない場合は、HP ProtectTools Security Manager によって必ずクエスチョン マーク付きの指紋画像が表示されます。このオプションを選択解除して、この画像の表示を無効にできます。

データのバックアップおよび復元

HP ProtectTools Security Manager のデータは定期的にバックアップすることをおすすめします。バックアップの頻度は、データが変更される頻度によって決まります。たとえば、毎日のように新しいログオンを追加している場合は、データを毎日バックアップする必要があります。

また、他のコンピューターへの移行時にバックアップを使用することもできます。この作業は、インポートおよびエクスポートと呼ばれます。

注記： この機能によってバックアップされるのはデータのみです。

バックアップ ファイルからデータを復元できるようにするには、バックアップ データを取り込むコンピューターに HP ProtectTools Security Manager をインストールしておく必要があります。

データをバックアップするには、以下の操作を行います。

1. 左側のパネルで、**[詳細設定]**→**[バックアップおよび復元]**の順にクリックします。
2. **[データのバックアップ]**をクリックします。
3. バックアップに含めるモジュールを選択します。多くの場合、すべてのモジュールの選択が必要になります。
4. ストレージ ファイルの名前を入力します。初期設定では、このファイルはユーザーの[ドキュメント]フォルダーに保存されます。別の場所を指定するには、**[参照]**をクリックします。
5. ファイルを保護するためのパスワードを入力します。
6. ID を検証します。
7. **[完了]**をクリックします。

データを復元するには、以下の操作を行います。

1. 左側のパネルで、**[詳細設定]**→**[バックアップおよび復元]**の順にクリックします。
2. **[データの復元]**をクリックします。
3. 以前に作成したストレージ ファイルを選択します。表示されているフィールドにパスを入力して、**[編集]**をクリックします。
4. ファイルを保護するために使用しているパスワードを入力します。

5. データを復元するモジュールを選択します。多くの場合、一覧表示されているすべてのモジュールを選択することになります。

6. **[完了]**をクリックします。

アプリケーションの追加

このプログラムに新しい機能を提供する、追加アプリケーションを利用できます。

[HP ProtectTools Security Manager]ダッシュボードで、**[[＋]他を検出]**をクリックして追加アプリケーションを検索します。

注記： ダッシュボードの左上隅に**[[＋]他を検出]**リンクがない場合は、このコンピューターの管理者によって無効に設定されています。

セキュリティ アプリケーションの状態

[Security Manager アプリケーションの状態]ページには、インストールされているセキュリティ アプリケーションの全体的な状態が表示されます。また、セットアップされているアプリケーション、および各アプリケーションのセットアップ状態が表示されます。この概要情報は、[HP ProtectTools Security Manager]ダッシュボードを開くか**[セキュリティ アプリケーション]**をクリックすると、自動的に表示されます。

7 Drive Encryption for HP ProtectTools（一部のモデルのみ）

△ **注意：** Drive Encryption モジュールをアンインストールする場合は、まず、暗号化されたすべてのドライブの暗号化を解除する必要があります。そうしないと、Drive Encryption 復元サービスに登録していない限り、暗号化されたドライブ上のデータにアクセスできなくなります。Drive Encryption モジュールを再インストールしても、暗号化されたドライブにはアクセスできません。

Drive Encryption for HP ProtectTools は、コンピューターのハードドライブを暗号化することによって完全なデータ保護を可能にします。Drive Encryption を有効にしている場合は、Windows オペレーティング システムが起動する前に表示される、Drive Encryption のログイン画面からログインする必要があります。

HP ProtectTools セットアップ ウィザードを使用すると、Windows 管理者は、Drive Encryption の有効化、暗号化キーのバックアップ、ユーザーの追加と削除、および Drive Encryption の無効化を行えます。詳しくは、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）ソフトウェアのヘルプを参照してください。

Drive Encryption では、以下のタスクを実行できます。

- 暗号化の管理
  - 個々のドライブの暗号化または暗号化の解除

    注記： 暗号化できるドライブは内蔵ハードドライブのみです。
- 復元
  - バックアップ キーの作成
  - 復元の実行

セットアップ手順

Drive Encryption を開く

1. **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. 左側の枠内で、**[Drive Encryption]**をクリックします。

一般的なタスク

Drive Encryption の有効化

Drive Encryption を有効にするには、HP ProtectTools セットアップ ウィザードを使用します。

注記： このウィザードは、ユーザーの追加および削除にも使用します。

または

1. **[スタート]→[すべてのプログラム]→[HP]→[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. 左側の枠内で、**[セキュリティ]→[機能]**の順にクリックします。
3. **[Drive Encryption]**チェック ボックスにチェックを入れ、**[次へ]**をクリックします。
4. **[暗号化するドライブ]**で、暗号化するハードドライブのチェック ボックスにチェックを入れます。
5. 適切なスロットにストレージ デバイスを挿入します。

   注記： 暗号化キーを保存するには、FAT32 でフォーマットされた USB ストレージ デバイスを使用する必要があります。

6. **[暗号化キーを保存する外付けストレージ デバイス]**で、暗号化キーを保存するストレージ デバイスのチェック ボックスにチェックを入れます。
7. **[適用]**をクリックします。

   ドライブの暗号化が開始されます。

詳しくは、HP ProtectTools Security Manager ソフトウェアのヘルプを参照してください。

Drive Encryption の無効化

Drive Encryption を無効にするには、HP ProtectTools セットアップ ウィザードを使用します。詳しくは、HP ProtectTools Security Manager ソフトウェアのヘルプを参照してください。

または

1. **[スタート]→[すべてのプログラム]→[HP]→[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. 左側の枠内で、**[セキュリティ]→[機能]**の順にクリックします。
3. **[Drive Encryption]**チェック ボックスのチェックを外し、**[適用]**をクリックします。

   ドライブの復号化が開始されます。

Drive Encryption の有効化後のログイン

Drive Encryption が有効になり、ユーザー アカウントが登録された後でコンピューターを起動した場合、Drive Encryption のログイン画面からログインする必要があります。

注記： Windows 管理者が HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）で[ブート前セキュリティ]を有効にしている場合は、Drive Encryption のログイン画面ではなく、コンピューターが起動した直後にコンピューターにログインします。

1. ユーザー名をクリックし、Windows のパスワードまたは Java Card の PIN を入力するか、または登録した指の指紋を認証システムで読み取らせます。
2. **[OK]**をクリックします。

注記： Drive Encryption のログイン画面で復元キーを使用してログインする場合は、Windows のログイン画面で Windows のユーザー名を選択し、パスワードを入力することも要求されます。

ハードドライブの暗号化によるデータの保護

ハードドライブを暗号化することによってデータを保護するには、HP ProtectTools セットアップ ウィザードを使用します。

1. HP ProtectTools Security Manager で、**[ここから開始]**をクリックして、**[セキュリティ マネージャーのセットアップ]**アイコンをクリックします。HP ProtectTools Security Manager の機能を説明するデモンストレーションが始まります。（[Drive Encryption]ページから HP ProtectTools Security Manager を起動することもできます。）
2. 左側の枠内で、**[Drive Encryption]→[暗号化の管理]**の順にクリックします。
3. **[暗号化を変更する]**をクリックします。
4. 暗号化するドライブを 1 つ以上選択します。

   注記： ハードドライブを暗号化することを強くおすすめします。

暗号化の状態の表示

ユーザーは HP ProtectTools Security Manager で暗号化の状態を表示できます。

注記： ドライブの暗号化の状態を変更するには、[HP ProtectTools 管理者コンソール]を使用する必要があります。

1. HP ProtectTools Security Manager を起動します。
2. **[マイ データ]**で**[暗号化の状態]**をクリックします。

   Drive Encryption が有効になっている場合、ドライブの状態が以下のどれかのステータス コードで表示されます。

   - アクティブ
   - 非アクティブ
   - 暗号化されていない
   - 暗号化済み
   - 暗号化
   - 暗号化の解除

   ハードドライブの暗号化または暗号化解除を実行中、暗号化または暗号化解除が完了した割合および完了するまでの残り時間が進行状況バーに表示されます。

高度なタスク

Drive Encryption の管理（管理者のタスク）

管理者は、[暗号化の管理]ページで、Drive Encription の状態（有効または無効）の表示や変更、およびコンピューターに取り付けられているすべてのハードドライブの暗号化の状態の表示ができます。

- 状態が無効の場合、Drive Encryption は HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）を使用して Windows 管理者によって有効にされておらず、ハードドライブは保護されていません。Drive Encryption を有効にするには、HP ProtectTools Security Manager のセットアップ ウィザードを使用します。
- 状態が有効の場合、Drive Encryption は有効化され、設定されています。ドライブは、次のどれかの状態になっています。
  - 暗号化されていない
  - 暗号化済み
  - 暗号化
  - 暗号化の解除

個々のドライブの暗号化または暗号化の解除

コンピューター上の 1 つまたは複数のハードドライブを暗号化するか、またはすでに暗号化されているドライブの暗号化を解除するには、暗号化変更機能を使用します。

1. **[HP ProtectTools 管理者コンソール]**を開き、**[Drive Encryption]**→**[暗号化管理]**の順にクリックします。
2. **[暗号化を変更する]**をクリックします。
3. [暗号化を変更する]ダイアログ ボックスで、暗号化するか、または暗号化を解除する各ハードドライブの横にあるチェック ボックスにチェックを入れるか、またはチェックを外して、**[OK]**をクリックします。

注記： ドライブの暗号化または暗号化解除が行われている間、現在のセッションで処理が完了するまでの残り時間が進行状況バーに表示されます。暗号化中にコンピューターをシャットダウンするか、スリープまたはハイバネーションを開始し、その後起動しなおした場合、残り時間の表示はリセットされますが、実際の暗号化は直前に停止した場所から再開されます。残り時間と進行状況の表示がすばやく進み、現在の進行状況が反映されます。

バックアップおよび復元（管理者のタスク）

[復元]ページでは、管理者は暗号化キーをバックアップし、復元することができます。

[ローカルの Drive Encryption キー バックアップ]：Drive Encryption が有効になっているときに、暗号化キーをリムーバブル メディアにバックアップできます。

バックアップ キーの作成

暗号化されたドライブの暗号化キーをリムーバブル ストレージ デバイスにバックアップすることができます。

△ 注意： バックアップ キーを含むストレージ デバイスは必ず安全な場所に保管してください。パスワードを忘れたり、Java Card を紛失したりした場合に、このデバイスがハードドライブにアクセスする唯一の方法となります。

1. **[HP ProtectTools 管理者コンソール]**を開き、**[Drive Encryption]**→**[復元]**の順にクリックします。
2. **[キーをバックアップする]**をクリックします。
3. [バックアップ ディスクを選択してください]ページで、暗号化キーをバックアップするデバイスのチェック ボックスにチェックを入れ、**[次へ]**をクリックします。
4. 表示されるページの次のページに記載されている情報を読み、**[次へ]**をクリックします。選択したストレージ デバイスに暗号化キーが保存されます。
5. 確認ダイアログ ボックスが表示されたら、**[完了]**をクリックします。

復元の実行

パスワードを忘れてしまった場合に復元を実行するには、以下の操作を行います。

1. コンピューターの電源を入れます。
2. バックアップ キーが保管されているリムーバブル ストレージ デバイスを装着します。
3. Drive Encryption for HP ProtectTools のログイン ダイアログ ボックスが表示されたら、**[キャンセル]**をクリックします。
4. 画面の左下隅にある**[オプション]**をクリックしてから、**[復元]**をクリックします。
5. バックアップ キーが含まれているファイルを選択するか、**[参照]**をクリックして該当のファイルを探してから、**[次へ]**をクリックします。
6. 確認ダイアログ ボックスが表示されたら、**[OK]**をクリックします。

   コンピューターが起動します。

注記： 復元を実行した後は、パスワードを再設定することを強くおすすめします。

8 Privacy Manager for HP ProtectTools（一部のモデルのみ）

Privacy Manager for HP ProtectTools を使用すると、電子メール、Microsoft Office ドキュメント、またはインスタント メッセージ（IM）を使用するときに、高度なセキュリティ ログイン（認証）方法を使用して、通信の発信元、整合性、セキュリティを確認できます。

Privacy Manager では、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）が提供するセキュリティ インフラストラクチャを活用します。HP ProtectTools セキュリティ マネージャーのセキュリティ ログイン方法は、以下のとおりです。

- 指紋認証
- Windows のパスワード
- HP ProtectTools Java Card

Privacy Manager では、上記のセキュリティ ログイン方法を使用できます。

Privacy Manager には、以下のものが必要です。

- HP ProtectTools セキュリティ マネージャー 5.00 以降
- Windows 7、Windows Vista®、または Windows XP のオペレーティング システム
- Microsoft Outlook 2007 または Microsoft Outlook 2003
- 有効な電子メール アカウント

注記： セキュリティ機能を使用するには、Privacy Manager から Privacy Manager の証明書というデジタル証明書を要求し、インストールしておく必要があります。Privacy Manager の証明書の要求について詳しくは、43 ページの 「Privacy Manager の証明書の要求とインストール」を参照してください。

セットアップ手順

Privacy Manager の起動

Privacy Manager を起動するには、以下の操作を行います。

1. **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools Security Manager]**の順にクリックします。
2. **[Privacy Manager]**をクリックします。

または

タスクバーの右端の通知領域にある**[HP ProtectTools]**アイコンを右クリックしてから**[Privacy Manager]**→**[構成]**の順にクリックします。

または

Microsoft Outlook の電子メール メッセージのツールバーで**[安全に送信]**の横にある下向きの矢印をクリックしてから、**[証明書]**または**[信頼済み連絡先]**をクリックします。

または

Microsoft Office ドキュメントのツールバーで**[署名と暗号化]**の横にある下向きの矢印をクリックしてから、**[証明書]**または**[信頼済み連絡先]**をクリックします。

Privacy Manager の証明書の管理

Privacy Manager の証明書は、公開キー基盤（PKI）と呼ばれる暗号化技術を使用して、データとメッセージを保護します。PKI の利用にあたり、ユーザーは暗号キーと、証明機関（CA）が発行する Privacy Manager の証明書を取得する必要があります。認証を定期的に要求するのみのほとんどのデータ暗号化ソフトウェアや認証ソフトウェアとは異なり、Privacy Manager は、暗号キーを使用して電子メール メッセージや Microsoft Office ドキュメントに署名するたびに認証を要求します。Privacy Manager によって、重要な情報の保存と送信の処理が安全で確実なものとなります。

以下のタスクを実行できます。

- Privacy Manager の証明書を要求およびインストールする
- Privacy Manager の証明書の詳細を表示する
- Privacy Manager の証明書を更新する
- 使用できる証明書が複数ある場合に、Privacy Manager が初期設定で使用する Privacy Manager の証明書を指定する
- Privacy Manager の証明書を削除および廃止する（高度なタスク）

Privacy Manager の証明書の要求とインストール

Privacy Manager の機能を使用するには、有効な電子メール アドレスを使用して Privacy Manager から Privacy Manager の証明書を要求し、インストールしておく必要があります。この電子メール アドレスは、Privacy Manager の証明書を要求するコンピューターの Microsoft Outlook のアカウントとして設定する必要があります。

Privacy Manager の証明書の要求

1. Privacy Manager を開き、**[証明書]**をクリックします。
2. **[Privacy Manager の証明書の要求]**をクリックします。
3. [ようこそ]ページで、画面に表示される内容を確認してから**[次へ]**をクリックします。
4. [使用許諾契約]ページで、使用許諾契約の内容を確認します。
5. **[使用許諾契約の条件に同意する場合はチェック]**の隣のチェック ボックスにチェックが入っていることを確認してから、**[次へ]**をクリックします。
6. [証明書の詳細]ページで、求められた情報を入力してから**[次へ]**をクリックします。
7. [証明書の要求が承認されました]ページで、**[完了]**をクリックします。
8. **[OK]**をクリックして証明書を閉じます。

Microsoft Outlook に、Privacy Manager の証明書が添付された電子メールが届きます。

事前に割り当てられた Privacy Manager Corporate の証明書の取得

1. Microsoft Outlook に、Corporate Certificate が事前に割り当てられたことを示す電子メールが届いています。その電子メールを開きます。
2. **[入手]**をクリックします。
3. Microsoft Outlook に、Privacy Manager の証明書が添付された電子メールが届きます。
4. 証明書をインストールするには、44 ページの 「Privacy Manager の証明書のインストール」を参照してください。

Privacy Manager の証明書のインストール

1. Privacy Manager の証明書の添付された電子メールを受信したら、メールを開き、**[設定]**ボタンをクリックします。[設定]ボタンは、Microsoft Outlook 2007 の場合はメッセージの右下隅、Microsoft Outlook 2003 の場合は左上隅にあります。
2. 選択したセキュリティ ログイン方法で認証します。
3. [証明書がインストールされました]ページで、**[次へ]**をクリックします。
4. [証明書のバックアップ]ページで、バックアップ ファイルの保存先と名前を入力するか、または**[参照]**をクリックして保存先を探します。

△ 注意： ファイルはハードドライブ以外の場所に保存し、安全な場所に保管してください。本人以外はこのファイルを使用できません。また、Privacy Manager の証明書と、関連するキーを復元しなければならない場合には、このファイルが必要です。

5. パスワードの入力と確認を行い、**[次へ]**をクリックします。
6. 選択したセキュリティ ログイン方法で認証します。
7. 信頼済み連絡先の招待の処理を始める場合は、48 ページの 「Microsoft Outlook のアドレス帳を使用した信頼済み連絡先の追加」のトピックで、手順 2 から始まる画面の説明に沿って操作します。

   または

[キャンセル]をクリックすると、後で信頼済み連絡先を追加できます。詳しくは、47 ページの 「信頼済み連絡先の追加」を参照してください。

Privacy Manager の証明書の詳細の表示

1. Privacy Manager を開き、**[証明書]**をクリックします。
2. Privacy Manager の証明書をクリックします。
3. **[証明書の詳細]**をクリックします。
4. 詳細の確認を終えたら、**[OK]**をクリックします。

Privacy Manager の証明書の更新

Privacy Manager の証明書が有効期限に近づくと、更新が必要であることが通知されます。

1. Privacy Manager を開き、**[証明書]**をクリックします。
2. **[証明書の更新]**をクリックします。
3. 画面の説明に沿って操作し、新しい Privacy Manager の証明書を購入します。

注記： Privacy Manager の証明書の更新処理を行っても、古い Privacy Manager の証明書は置き換えられません。新しい Privacy Manager の証明書を購入したら、43 ページの 「Privacy Manager の証明書の要求とインストール」に記載されている手順でインストールする必要があります。

Privacy Manager の証明書の初期設定の指定

お使いのコンピューターに別の証明機関からの証明書がインストールされている場合でも、Privacy Manager には Privacy Manager の証明書のみが表示されます。

コンピューターに Privacy Manager からインストールした Privacy Manager の証明書が複数ある場合は、どれか 1 つを初期設定の証明書として指定できます。

1. Privacy Manager を開き、**[証明書]**をクリックします。
2. 初期設定として使用する Privacy Manager の証明書をクリックしてから、**[初期値の指定]**をクリックします。
3. **[OK]**をクリックします。

注記： 初期設定の Privacy Manager の証明書をいつも使用する必要はありません。Privacy Manager のさまざまな機能によって、使用する Privacy Manager の証明書を選択できます。

Privacy Manager の証明書の削除

Privacy Manager の証明書を削除すると、この証明書で暗号化したファイルを開いたり、データを表示したりすることができなくなります。間違えて Privacy Manager の証明書を削除した場合は、証明書のインストール時に作成したバックアップ ファイルを使用して証明書を復元できます。詳しくは、46 ページの 「Privacy Manager の証明書の復元」を参照してください。

Privacy Manager の証明書を削除するには、以下の操作を行います。

1. Privacy Manager を開き、**[証明書]**をクリックします。
2. 削除する Privacy Manager の証明書をクリックしてから、**[詳細]**をクリックします。

3. **[削除]**をクリックします。

4. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

5. **[閉じる]**をクリックし、**[適用]**をクリックします。

Privacy Manager の証明書の復元

Privacy Manager の証明書のインストール中に、証明書のバックアップ コピーを作成するよう要求されます。バックアップ コピーの作成は、[移行]ページからも実行できます。このバックアップ コピーは、別のコンピューターへの移行時や、証明書を同一のコンピューターに復元する場合に使用できます。

1. Privacy Manager を開き、**[移行]**をクリックします。

2. **[復元]**をクリックします。

3. [移行ファイル]ページで、**[参照]**をクリックし、バックアップ処理中に作成した.dppsm ファイルを探してから、**[次へ]**をクリックします。

4. バックアップ作成時に使用したパスワードを入力して、**[次へ]**をクリックします。

5. **[完了]**をクリックします。

6. **[OK]**をクリックします。

詳しくは、44 ページの 「Privacy Manager の証明書のインストール」、または61 ページの 「Privacy Manager の証明書および信頼済み連絡先のバックアップ」を参照してください。

Privacy Manager の証明書の廃止

お使いの Privacy Manager の証明書のセキュリティに問題があると感じる場合、その証明書を廃止できます。

注記： Privacy Manager の証明書を廃止しても、削除はされません。この証明書は、暗号化したファイルを表示するために引き続き使用できます。

1. Privacy Manager を開き、**[証明書]**をクリックします。

2. **[詳細]**をクリックします。

3. 廃止する Privacy Manager の証明書をクリックしてから、**[廃止]**をクリックします。

4. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

5. 選択したセキュリティ ログイン方法で認証します。

6. 画面に表示される説明に沿って操作します。

信頼済み連絡先の管理

信頼済み連絡先とは、安全に通信が出来るように、互いに Privacy Manager の証明書を交換したユーザーのことです。

Trusted Contacts Manager（信頼済み連絡先マネージャー）を使用すると、以下のタスクを実行できます。

- 信頼済み連絡先の詳細の表示
- 信頼済み連絡先の削除
- 信頼済み連絡先の廃止状態の確認（高度なタスク）

信頼済み連絡先の追加

信頼済み連絡先を追加するには、以下の 3 つの処理を行います。

1. 信頼済み連絡先の受信者に、電子メールで招待状を送信します。
2. 信頼済み連絡先の受信者が、この電子メールに返信します。
3. 信頼済み連絡先の受信者から返信メールを受け取ったら、**[承認]**をクリックします。

信頼済み連絡先の電子メール招待状は、個々の受信者宛てに送信することも、Microsoft Outlook のアドレス帳に記載されているすべての連絡先に送信することもできます。

以下を参照して、信頼済み連絡先を追加します。

注記： 信頼済み連絡先になるための招待状に返信するには、信頼済み連絡先の受信者のコンピューターに、Privacy Manager または別のクライアントがインストールされている必要があります。別のクライアントのインストールについて詳しくは、DigitalPersona の Web サイト http://DigitalPersona.com/PrivacyManager/（英語サイト）にアクセスしてください。

信頼済み連絡先の追加

1. Privacy Manager を開き、**[信頼済み連絡先マネージャー]**→**[連絡先の招待]**の順にクリックします。

   または

   Microsoft Outlook で、ツールバーの**[安全に送信]**の横にある下向きの矢印をクリックしてから、**[連絡先の招待]**をクリックします。
2. [証明書の選択]ダイアログ ボックスが表示された場合は、使用する Privacy Manager の証明書をクリックしてから**[OK]**をクリックします。
3. [信頼済み連絡先の招待]ダイアログ ボックスが表示されたら、画面に表示されている内容を確認してから**[OK]**をクリックします。

   自動的に電子メールが生成されます。
4. 信頼済み連絡先に追加する受信者の電子メール アドレスを、1 つ以上入力します。
5. テキストを編集し、自分の名前を署名します（オプション）。
6. **[送信]**をクリックします。

   注記： Privacy Manager の証明書を取得していない場合、信頼済み連絡先要求の送信には Privacy Manager の証明書が必要というメッセージが表示されます。**[OK]**をクリックして、[証明書の要求ウィザード]）を起動します。詳しくは、43 ページの 「Privacy Manager の証明書の要求とインストール」を参照してください。
7. 選択したセキュリティ ログイン方法で認証します。

注記： 信頼済み連絡先の受信者は、電子メールを受信すると、電子メールを開いて右下隅の**[承認]**をクリックし、確認用のダイアログ ボックスが表示されたら**[OK]**をクリックする必要があります。

8. 信頼済み連絡先になるための招待を承認した返信メールを受信者から受け取ったら、電子メール右下隅の**[承認]**をクリックします。

   ダイアログ ボックスが開き、受信者が信頼済み連絡先の一覧に正常に追加されたことを確認できます。

9. **[OK]**をクリックします。

Microsoft Outlook のアドレス帳を使用した信頼済み連絡先の追加

1. Privacy Manager を開き、**[信頼済み連絡先マネージャー]**→**[連絡先の招待]**の順にクリックします。

   または

   Microsoft Outlook で、ツールバーの**[安全に送信]**の横にある下向きの矢印をクリックしてから、**[[Microsoft Outlook]のすべての連絡先を招待]**をクリックします。

2. [信頼済み連絡先の招待]ページが開いたら、信頼済み連絡先に追加する受信者の電子メール アドレスを選択してから**[次へ]**をクリックします。

3. [招待状の送信]ページが開いたら、**[完了]**をクリックします。

   選択した Microsoft Outlook の電子メール アドレスを一覧表示した電子メールが自動生成されます。

4. テキストを編集し、自分の名前を署名します（オプション）。

5. **[送信]**をクリックします。

   注記： Privacy Manager の証明書を取得していない場合、信頼済み連絡先要求の送信には Privacy Manager の証明書が必要というメッセージが表示されます。**[OK]**をクリックして、[証明書の要求ウィザード]を起動します。詳しくは、43 ページの 「Privacy Manager の証明書の要求とインストール」を参照してください。

6. 選択したセキュリティ ログイン方法で認証します。

   注記： 信頼済み連絡先の受信者は、電子メールを受信すると、電子メールを開いて右下隅の**[承認]**をクリックし、確認用のダイアログ ボックスが表示されたら**[OK]**をクリックする必要があります。

7. 信頼済み連絡先になるための招待を承認した返信メールを受信者から受け取ったら、電子メール右下隅の**[承認]**をクリックします。

   ダイアログ ボックスが開き、受信者が信頼済み連絡先の一覧に正常に追加されたことを確認できます。

8. **[OK]**をクリックします。

信頼済み連絡先の詳細の表示

1. Privacy Manager を開き、**[信頼済み連絡先]**をクリックします。

2. 信頼済み連絡先をクリックします。

3. **[連絡先の詳細]**をクリックします。

4. 詳細の確認を終えたら、**[OK]**をクリックします。

信頼済み連絡先の削除

1. Privacy Manager を開き、**[信頼済み連絡先]**をクリックします。

2. 削除する信頼済み連絡先をクリックします。

3. **[連絡先の削除]**をクリックします。

4. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

信頼済み連絡先の廃止状態の確認

信頼済み連絡先が自身の Privacy Manager の証明書を廃止しているかどうかを確認するには、以下の操作を行います。

1. Privacy Manager を開き、**[信頼済み連絡先]**をクリックします。

2. 信頼済み連絡先をクリックします。

3. **[詳細]**ボタンをクリックします。

   [高度な信頼済み連絡先管理]ダイアログ ボックスが開きます。

4. **[廃止の確認]**をクリックします。

5. **[閉じる]**をクリックします。

一般的なタスク

Privacy Manager は、以下の Microsoft 製品で使用できます。

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger for Windows Vista

Microsoft Outlook での Privacy Manager の使用

Privacy Manager をインストールすると、Microsoft Outlook のツールバーに[プライバシ]ボタンが表示されるようになります。また、Microsoft Outlook の各電子メール メッセージのツールバーに[安全に送信]ボタンが表示されるようになります。**[プライバシ]**または**[安全に送信]**の横にある下向き矢印をクリックすると、以下のオプションを選択できます。

- [署名して送信]（[安全に送信]ボタンのみ）：このオプションを使用すると、電子メールにデジタル署名が付加されます。この電子メールは、選択したセキュリティ ログイン方法による認証の後に送信されます。
- [信頼済み連絡先宛てに封印して送信]（[安全に送信]ボタンのみ）：このオプションを使用すると、電子メールにデジタル署名が付加され、電子メールが暗号化されます。この電子メールは、選択したセキュリティ ログイン方法による認証の後に送信されます。
- [連絡先の招待]：このオプションを使用すると、信頼済み連絡先の招待状を送信できます。詳しくは、47 ページの 「信頼済み連絡先の追加」を参照してください。
- [Outlook のすべての連絡先を招待]：このオプションを使用すると、Microsoft Outlook のアドレス帳に記載されているすべての連絡先に信頼済み連絡先の招待状を送信できます。詳しくは、48 ページの 「Microsoft Outlook のアドレス帳を使用した信頼済み連絡先の追加」を参照してください。
- [Privacy Manager ソフトウェアを開く]：証明書、信頼済み連絡先、および[設定]オプションを使用すると、Privacy Manager ソフトウェアを開いて現在の設定の追加、表示、または変更ができます。詳しくは、50 ページの 「Microsoft Outlook 用の Privacy Manager の設定」を参照してください。

Microsoft Outlook 用の Privacy Manager の設定

1. Privacy Manager を開き、**[設定]**をクリックしてから**[電子メール]**タブをクリックします。

   または

   Microsoft Outlook のメインのツールバーで、**[安全に送信]**（Microsoft Outlook 2003 の**[プライバシ]**）の横にある下向きの矢印をクリックしてから**[設定]**をクリックします。

   または

   Microsoft の電子メール メッセージのツールバーで、**[安全に送信]**の横にある下向きの矢印をクリックしてから**[設定]**をクリックします。

2. 安全な電子メールを送信するときに実行する操作を選択し、**[OK]**をクリックします。

電子メール メッセージの署名および送信

1. Microsoft Outlook で、**[新規作成]**または**[返信]**をクリックします。
2. 電子メール メッセージを入力します。
3. **[安全に送信]**（Microsoft Outlook 2003 の**[プライバシ]**）の横にある下向きの矢印をクリックしてから、**[署名して送信]**をクリックします。
4. 選択したセキュリティ ログイン方法で認証します。

電子メール メッセージの封印および送信

デジタル処理によって署名、封印（暗号化）されている、封印された電子メールを閲覧できるのは、信頼済み連絡先の一覧から選択したユーザーのみです。

電子メールを封印して信頼済み連絡先に送信するには、以下の操作を行います。

1. Microsoft Outlook で、**[新規作成]**または**[返信]**をクリックします。
2. 電子メール メッセージを入力します。
3. **[安全に送信]**（Microsoft Outlook 2003 の**[プライバシ]**）の横にある下向きの矢印をクリックしてから、**[信頼済み連絡先宛てに封印して送信]**をクリックします。
4. 選択したセキュリティ ログイン方法で認証します。

封印された電子メール メッセージの表示

封印された電子メール メッセージを開くと、電子メールの見出しにセキュリティ ラベルが表示されます。このセキュリティ ラベルには、以下の情報が記載されています。

- 電子メールに署名した人物の身元確認に使用された証明書
- 電子メールに署名した人物の証明書の確認に使用された製品

Microsoft Office 2007 ドキュメントでの Privacy Manager の使用

注記： Privacy Manager は、Microsoft Office 2007 ドキュメントでのみ使用できます。

Privacy Manager の証明書をインストールすると、Microsoft Word、Microsoft Excel、および Microsoft PowerPoint のすべてのドキュメントのツールバーの右側に、[署名と暗号化]ボタンが表示されます。**[署名と暗号化]**の横にある下向き矢印をクリックすると、以下のオプションを選択できます。

- [ドキュメントへの署名]：このオプションを使用すると、ドキュメントにデジタル署名が付加されます。
- [署名の前に署名欄を追加]（Microsoft Word と Microsoft Excel のみ）：初期設定では、Microsoft Word または Microsoft Excel のドキュメントに対する署名や暗号化が行われると、署名欄が追加されます。このオプションをオフにするには、**[署名欄の追加]**をクリックしてチェック マークを外します。
- [ドキュメントの暗号化]：このオプションを使用すると、ドキュメントにデジタル署名が付加され、ドキュメントが暗号化されます。

- [暗号化の解除]：このオプションを使用すると、ドキュメントの暗号化が解除されます。
- [Privacy Manager ソフトウェアを開く]：証明書、信頼済み連絡先、および[設定]オプションを使用すると、Privacy Manager ソフトウェアを開いて現在の設定の追加、表示、または変更ができます。詳しくは、43 ページの 「Privacy Manager の証明書の管理」、46 ページの 「信頼済み連絡先の管理」、または52 ページの 「Microsoft Office 用の Privacy Manager の設定」を参照してください。

Microsoft Office 用の Privacy Manager の設定

1. Privacy Manager を開き、**[設定]**をクリックしてから**[ドキュメント]**タブをクリックします。

   または

   Microsoft Office ドキュメントのツールバーで、**[署名と暗号化]**の横にある下向きの矢印をクリックしてから**[設定]**をクリックします。

2. 設定する操作を選択し、**[OK]**をクリックします。

Microsoft Office ドキュメントへの署名

1. Microsoft Word、Microsoft Excel、または Microsoft PowerPoint でドキュメントを作成し、保存します。
2. **[署名と暗号化]**の横にある下向きの矢印をクリックしてから、**[ドキュメントへの署名]**をクリックします。
3. 選択したセキュリティ ログイン方法で認証します。
4. 確認用のダイアログ ボックスが表示されたら、画面に表示されている内容を確認してから**[OK]**をクリックします。

後でドキュメントを編集する場合は、以下の操作を行います。

1. 画面の左上隅にある**[Office]**ボタンをクリックします。
2. **[準備]**→**[最終版としてマーク]**の順にクリックします。
3. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックして作業を続けます。
4. 編集が終わったら、再びドキュメントに署名します。

Microsoft Word または Microsoft Excel ドキュメント署名時の署名欄の追加

Privacy Manager では、Microsoft Word または Microsoft Excel ドキュメントに署名する場合に署名欄を追加できます。

1. Microsoft Word または Microsoft Excel でドキュメントを作成し、保存します。
2. **[ホーム]**メニューをクリックします。
3. **[署名と暗号化]**の横にある下向きの矢印をクリックしてから、**[署名の前に署名欄を追加]**をクリックします。

   注記： このオプションを選択すると、[署名の前に署名欄を追加]の横にチェック マークが表示されます。初期設定では、このオプションは有効になっています。

4. **[署名と暗号化]**の横にある下向きの矢印をクリックしてから、**[ドキュメントへの署名]**をクリックします。

5. 選択したセキュリティ ログイン方法で認証します。

Microsoft Word または Microsoft Excel ドキュメントに、推奨する署名者を追加する

推奨する署名者を指名することによって、ドキュメントに複数の署名欄を追加できます。推奨する署名者とは、ドキュメントに署名欄を追加するために Microsoft Word または Microsoft Excel ドキュメントの所有者が指名したユーザーのことです。推奨する署名者には自分自身を指名することも、別の人物を指名してドキュメントへの署名を依頼することもできます。たとえば、部署内の全員の署名が必要なドキュメントを準備する場合、特定の日付で署名するよう指示した全員分の署名欄を、ドキュメントの最終ページの最下部に設けることができます。

Microsoft Word または Microsoft Excel ドキュメントに、推奨する署名者を追加するには、以下の操作を行います。

1. Microsoft Word または Microsoft Excel でドキュメントを作成し、保存します。

2. **[挿入]**メニューをクリックします。

3. ツールバーの**[テキスト]**グループで、**[署名欄]**の横にある矢印をクリックしてから**[Privacy Manager 署名プロバイダー]**をクリックします。

   [署名の設定]ダイアログ ボックスが表示されます。

4. ボックス内の**[推奨する署名者]**の下に、推奨する署名者の名前を入力します。

5. ボックス内の**[署名者への指示]**の下に、この推奨する署名者へのメッセージを入力します。

   注記： このメッセージはタイトルとして表示されますが、ドキュメントに署名すると、削除したりユーザーのタイトルに置き換えたりすることができます。

6. **[署名欄に署名日を表示]**チェック ボックスにチェックを入れて、日付を表示します。

7. **[署名欄に署名者のタイトルを表示]**チェック ボックスにチェックを入れて、タイトルを表示します。

   注記： ドキュメントの所有者が、推奨する署名者を自身のドキュメントに割り当てているため、**[署名欄に署名日を表示]**および**[署名欄に署名者のタイトルを表示]**の各チェック ボックスにチェックが入っていないと、推奨する署名者は署名欄に日付やタイトルを表示できません。これには推奨する署名者によるドキュメント設定は関係しません。

8. **[OK]**をクリックします。

推奨する署名者の署名欄の追加

推奨する署名者がドキュメントを開くと、自分の名前が角かっこで囲まれて表示され、署名を求められていることがわかります。

ドキュメントに署名するには、以下の操作を行います。

1. 適切な署名欄をダブルクリックします。

2. 選択したセキュリティ ログイン方法で認証します。

   ドキュメントの所有者が指定した設定に沿って、署名欄が表示されます。

Microsoft Office ドキュメントの暗号化

自分自身と信頼済み連絡先のために、Microsoft Office ドキュメントを暗号化できます。ドキュメントを暗号化してから閉じると、自分自身と一覧から選択した信頼済み連絡先は、このドキュメントを開くときに認証が必要となります。

Microsoft Office ドキュメントを暗号化するには、以下の操作を行います。

1. Microsoft Word、Microsoft Excel、または Microsoft PowerPoint でドキュメントを作成し、保存します。
2. **[ホーム]**メニューをクリックします。
3. **[署名と暗号化]**の横にある下向き矢印をクリックしてから、**[ドキュメントの暗号化]**をクリックします。

   [信頼済み連絡先の選択]ダイアログ ボックスが表示されます。
4. ドキュメントを開いて内容を閲覧できるようにする信頼済み連絡先の名前をクリックします。

   注記： 信頼済み連絡先の名前を複数選択するには、ctrl キーを押しながら個々の名前をクリックします。
5. **[OK]**をクリックします。

後でドキュメントを編集する場合は、54 ページの 「Microsoft Office ドキュメントの暗号化の解除」に記載されている手順で操作します。暗号化を解除すると、ドキュメントを編集できます。再びドキュメントを暗号化するには、ここに記載されている手順で操作します。

Microsoft Office ドキュメントの暗号化の解除

Microsoft Office ドキュメントの暗号化を解除すると、自分自身と信頼済み連絡先は、認証なしでこのドキュメントを開いて内容を閲覧できるようになります。

Microsoft Office ドキュメントの暗号化を解除するには、以下の操作を行います。

1. 暗号化された Microsoft Word、Microsoft Excel、または Microsoft PowerPoint ドキュメントを開きます。
2. 選択したセキュリティ ログイン方法で認証します。
3. **[ホーム]**メニューをクリックします。
4. **[署名と暗号化]**の横にある下向き矢印をクリックしてから、**[暗号化の解除]**をクリックします。

暗号化された Microsoft Office ドキュメントの送信

電子メール メッセージに、暗号化された Microsoft Office ドキュメントを添付できます。電子メール自体への署名や暗号化は不要です。これには、ファイルを添付した一般の電子メールの場合と同様に、署名または暗号化したドキュメントを添付した電子メールを作成し、送信します。

ただし、最適なセキュリティのため、署名または暗号化された Microsoft Office ドキュメントを添付する場合には、電子メールを暗号化することをおすすめします。

署名および暗号化した Microsoft Office ドキュメントを添付して、封印した電子メールを送信するには、以下の操作を行います。

1. Microsoft Outlook で、**[新規作成]**または**[返信]**をクリックします。
2. 電子メール メッセージを入力します。
3. Microsoft Office ドキュメントを添付します。
4. 詳しい手順については、51 ページの 「電子メール メッセージの封印および送信」を参照してください。

署名付き Microsoft Office ドキュメントの表示

注記： 署名付き Microsoft Office ドキュメントを表示するには、Privacy Manager の証明書は不要です。

署名付き Microsoft Office ドキュメントを開くと、ドキュメント ウィンドウ下部のステータス バーに[デジタル署名]アイコンが表示されます。

1. **[デジタル署名]**アイコンをクリックすると、[署名]ダイアログの表示が切り替わります。このダイアログには、ドキュメントに署名したすべてのユーザー名とその個々の署名日が表示されます。
2. 個々の署名の詳細を表示するには、[署名]ダイアログで名前を右クリックして[署名の詳細]を選択します。

暗号化された Microsoft Office ドキュメントの表示

暗号化された Microsoft Office ドキュメントを別のコンピューターから閲覧するには、そのコンピューターに Privacy Manager をインストールしておく必要があります。また、ファイルの暗号化に使用した Privacy Manager の証明書を復元する必要があります。

信頼済み連絡先が暗号化された Microsoft Office ドキュメントを閲覧するには、Privacy Manager の証明書が必要です。なお、コンピューターに Privacy Manager をインストールしておく必要があります。また、暗号化された Microsoft Office ドキュメントの所有者が、この信頼済み連絡先を選択している必要があります。

Windows Live Messenger での Privacy Manager の使用

Privacy Manager は、以下の安全な通信機能を Windows Live Messenger に追加します。

- **安全なチャット**：メッセージは、SSL/TLS（Secure Sockets Layer/Transport Layer Security）を使用して、XML プロトコルで送信されます。これは、電子商取引のセキュリティ確保のための技術と同じです。
- **受信者の識別**：メッセージを送信する前に、相手の存在と身元を確認できます。
- **署名付きメッセージ**：メッセージに電子署名を付加できます。メッセージが改ざんされると、受信者がメッセージを受け取ったときに、無効なメッセージとしてマークされます。
- **非表示/表示の機能**：[Privacy Manager Chat]ウィンドウで、特定のメッセージまたはすべてのメッセージを非表示にできます。内容が非表示になっているメッセージを送信することもできます。このメッセージを表示するには、認証が必要です。

- **安全なチャットの履歴**：チャット セッションの記録は保存前に暗号化され、閲覧するには認証が必要です。
- **自動ロック/ロック解除**：[Privacy Manager Chat]ウィンドウのロックとロック解除ができます。また、操作のない状態が指定の時間を超えると自動的にロックされるように設定できます。

Privacy Manager Chat セッションの開始

注記： Privacy Manager Chat を使用するには、双方に Privacy Manager と Privacy Manager の証明書がインストールされている必要があります。Privacy Manager の証明書のインストールについて詳しくは、43 ページの 「Privacy Manager の証明書の要求とインストール」を参照してください。

1. Windows Live Messenger で Privacy Manager Chat を始めるには、以下のどれかの手順で操作します。

   a. Windows Live Messenger でオンライン上の連絡相手を右クリックしてから、**[操作の開始]**を選択します。

   b. **[チャットを開始する]**をクリックします。

   または

   a. Windows Live Messenger でオンライン上の連絡相手をダブルクリックしてから、**[動作の一覧を参照する]**メニューをクリックします。

   b. **[アクション]→[チャットを開始する]**の順にクリックします。

   または

   a. 通知領域にある[ProtectTools]アイコンを右クリックし、**[Privacy Manager for HP ProtectTools]→[チャットを開始する]**の順にクリックします。

   b. Windows Live Messenger で、**[アクション:動作を開始する]**をクリックし、**[Privacy Manager Chat]**を選択します。

   注記： Windows Live Messenger では各ユーザーがオンラインである必要があり、ユーザーが互いの Windows Live Messenger のオンライン ウィンドウに表示されている必要があります。オンラインのユーザーをクリックして選択します。

   Privacy Manager Chat を始めるときには、Privacy Manager から連絡相手に招待状が送信されます。招待された相手が承認すると、[Privacy Manager Chat]ウィンドウが開きます。招待された相手が Privacy Manager を持っていない場合は、ダウンロードするよう要求されます。

2. **[開始]**をクリックすると、安全なチャットが始まります。

Windows Live Messenger 用の Privacy Manager の設定

1. Privacy Manager Chat で、**[設定]**ボタンをクリックします。

   または

   Privacy Manager で、**[設定]**をクリックしてから**[チャット]**タブをクリックします。

   または

   Privacy Manager Live Messenger History Viewer で、**[設定]**ボタンをクリックします。

2. セッションをロックするまでの Privacy Manager Chat の待機時間を指定するには、**[操作しない状態が_分の経過でセッションをロック]**ボックスで数を選択します。

3. チャット セッションの履歴フォルダーを指定するには、**[参照]**をクリックしてフォルダーを探してから、**[OK]**をクリックします。

4. セッションを閉じるときに自動的にセッションを暗号化して保存するには、**[安全なチャット履歴を自動的に保存]**チェック ボックスにチェックを入れます。

5. **[OK]**をクリックします。

[Privacy Manager Chat]ウィンドウでのチャット

Privacy Manager Chat を開始すると、Windows Live Messenger で[Privacy Manager Chat]ウィンドウが開きます。Privacy Manager Chat の使い方は、一般的な Windows Live Messenger の使い方と同様です。ただし、以下の機能は[Privacy Manager Chat]ウィンドウでのみ利用できます。

- **[保存]**：このボタンをクリックすると、設定時に指定したフォルダーにチャット セッションが保存されます。セッションを閉じるたびに自動的に保存するよう Privacy Manager Chat を設定することもできます。
- **[すべて非表示]**と**[すべて表示]**：各ボタンをクリックすると、[セキュア通信]ウィンドウに表示されているメッセージが展開されたり折りたたまれたりします。メッセージのヘッダーをクリックして、個々のメッセージの非表示と表示を切り替えることもできます。
- **[相手確認]**：このボタンをクリックすると、相手からの認証が要求されます。
- **[ロック]**：このボタンをクリックすると、[Privacy Manager Chat]ウィンドウが閉じて[チャットの登録]ウィンドウに戻ります。再び[セキュア通信]ウィンドウを表示するには、**[セッションの再開]**をクリックし、選択したセキュリティ ログイン方法で認証します。
- **[送信]**：このボタンをクリックすると、暗号化されたメッセージが相手に送信されます。
- **[署名して送信]**：このチェック ボックスにチェックを入れると、メッセージに電子署名が付加され、メッセージが暗号化されます。メッセージが改ざんされると、受信者がメッセージを受け取ったときに、無効なメッセージとしてマークされます。署名付きメッセージを送信するたびに認証が必要です。
- **[非表示で送信]**：このチェック ボックスにチェックを入れるとメッセージが暗号化され、メッセージの見出しのみを表示して送信されます。相手がメッセージの内容を読むには、認証する必要があります。

チャット履歴の表示

Privacy Manager Chat：Live Messenger History Viewer には、暗号化された Privacy Manager Chat セッション ファイルが表示されます。セッションは、[Privacy Manager Chat]ウィンドウの**[保存]**をクリックするか、Privacy Manager の[チャット]タブで自動保存を設定することによって保存されます。このビューアーには、セッションごとに、（暗号化された）連絡先のスクリーン名と、セッションの開始日時と終了日時が表示されます。初期設定では、設定したすべての電子メール アカウントのセッションが表示されます。**[履歴を表示]**メニューを使用すると、特定のアカウントのみを選択して表示できます。

このビューアーでは、以下のタスクを実行できます。

- 58 ページの 「すべてのセッションの公開」
- 58 ページの 「特定のアカウントのセッションの公開」
- 58 ページの 「セッション ID の表示」
- 59 ページの 「セッションの表示」

- 59 ページの 「テキストの指定によるセッションの検索」
- 59 ページの 「セッションの削除」
- 59 ページの 「列の追加または削除」
- 60 ページの 「表示中のセッションのフィルタリング」

Live Messenger History Viewer を起動するには、以下の操作を行います。

▲ タスクバーの右端の通知領域にある**[HP ProtectTools]**アイコンを右クリックして、**[Privacy Manager: for HP ProtectTools]**→**[Live Messenger History Viewer]**の順にクリックします。

または

▲ チャット セッションで、**[履歴ビューアー]**または**[履歴]**をクリックします。

すべてのセッションの公開

すべてのセッションを公開すると、選択中のセッション（複数可）と、同一アカウントのすべてのセッションについて、暗号化された Contact Screen Name が表示されます。

保存したすべてのチャット履歴セッションを公開するには、以下の操作を行います。

1. Live Messenger History Viewer で、任意のセッションを右クリックしてから**[すべてのセッションの公開]**を選択します。
2. 選択したセキュリティ ログイン方法で認証します。

   Contact Screen Name の暗号化が解除されます。
3. 任意のセッションをダブルクリックして、内容を表示します。

特定のアカウントのセッションの公開

セッションを公開すると、選択中のセッションの暗号化された Contact Screen Name が表示されます。

特定のチャット履歴セッションを公開するには、以下の操作を行います。

1. Live Messenger History Viewer で、任意のセッションを右クリックしてから**[セッションの公開]**を選択します。
2. 選択したセキュリティ ログイン方法で認証します。

   Contact Screen Name の暗号化が解除されます。
3. 公開されたセッションをダブルクリックして、内容を表示します。

注記： 同じ証明書で暗号化された別のセッションは、開錠されたアイコンで表示されます。これらのセッションは、認証しないでダブルクリックするだけで表示できます。別の証明書で暗号化されたセッションは、施錠されたアイコンで表示されます。これらのセッションの Contact Screen Name や内容を表示するには、別途認証が必要です。

セッション ID の表示

セッション ID を表示するには、以下の操作を行います。

▲ Live Messenger History Viewer で、任意の公開されたセッションを右クリックしてから**[セッション ID の表示]**を選択します。

セッションの表示

セッションを表示すると、表示用のファイルが開きます。セッションが公開されていなかった場合は（暗号化された Contact Screen Name が表示されます）、ここで公開されます。

Live Messenger の履歴セッションを表示するには、以下の操作を行います。

1. Live Messenger History Viewer で、任意のセッションを右クリックしてから**[表示]**を選択します。
2. 画面に指示が表示されたら、選択したセキュリティ ログイン方法で認証します。

   セッションの内容の暗号化が解除されます。

テキストの指定によるセッションの検索

ビューアーのウィンドウに表示されている、公開された（暗号化が解除された）セッションのテキストのみ検索ができます。これらのセッションでは、Contact Screen Name が平文で表示されています。

チャット履歴セッションのテキストを検索するには、以下の操作を行います。

1. Live Messenger History Viewer で、**[検索]**ボタンをクリックします。
2. 検索するテキストを入力し、検索パラメーターを設定してから**[OK]**をクリックします。

   テキストを含むセッションが、ビューアーのウィンドウに強調表示されます。

セッションの削除

1. チャット履歴セッションを選択します。
2. **[削除]**をクリックします。

列の追加または削除

初期設定では、Live Messenger History Viewer に、最もよく使用する列が 3 つ表示されます。列は画面に追加したり、画面から削除したりすることができます。

画面に列を追加するには、以下の操作を行います。

1. 任意の列見出しを右クリックしてから、**[列の追加と削除]**を選択します。
2. 左側のパネルの列見出しを選択してから**[追加]**をクリックして、列を右側のパネルに移動します。

画面から列を削除するには、以下の操作を行います。

1. 任意の列見出しを右クリックしてから、**[列の追加と削除]**を選択します。
2. 右側のパネルの列見出しを選択してから**[削除]**をクリックして、列を左側のパネルに移動します。

表示中のセッションのフィルタリング

Live Messenger History Viewer には、すべてのアカウントのセッションが一覧表示されます。表示中のセッションを、以下の条件でフィルタリングすることもできます。

- 特定のアカウント。詳しくは、60 ページの 「特定のアカウントのセッションの表示」を参照してください。
- 日付の範囲。詳しくは、60 ページの 「日付範囲内のセッションの表示」を参照してください。
- 別のフォルダー。詳しくは、60 ページの 「初期設定フォルダー以外のフォルダーに保存されているセッションの表示」を参照してください。

特定のアカウントのセッションの表示

▲ Live Messenger History Viewer で、**[履歴を表示]**メニューからアカウントを選択します。

日付範囲内のセッションの表示

1. Live Messenger History Viewer で、**[高度なフィルター]**アイコンをクリックします。

   [高度なフィルター]ダイアログ ボックスが表示されます。

2. **[指定した日付範囲内のセッションのみを表示]**を選択します。
3. **[以降の日]**と**[以前の日]**の各ボックスに年月日を入力するか、カレンダーの横の矢印をクリックして日付を選択します。
4. **[OK]**をクリックします。

初期設定フォルダー以外のフォルダーに保存されているセッションの表示

1. Live Messenger History Viewer で、**[高度なフィルター]**アイコンをクリックします。
2. **[別の履歴ファイル フォルダーを使用]**チェック ボックスにチェックを入れます。
3. フォルダーの場所を入力するか、**[参照]**をクリックしてフォルダーを探します。
4. **[OK]**をクリックします。

高度なタスク

別のコンピューターへの Privacy Manager の証明書と信頼済み連絡先の移行

Privacy Manager の証明書と信頼済み連絡先を、安全に別のコンピューターに移行したり、安全にデータをバックアップしたりできます。これには、Privacy Manager の証明書と信頼済み連絡先のバックアップをパスワードで保護されたファイルとしてネットワーク上の場所かリムーバブル ストレージ デバイスに作成してから、新しいコンピューターにこのファイルを復元します。

Privacy Manager の証明書および信頼済み連絡先のバックアップ

Privacy Manager の証明書と信頼済み連絡先をパスワードで保護されたファイルにバックアップするには、以下の操作を行います。

1. Privacy Manager を開き、**[移行]**をクリックします。
2. **[バックアップ]**をクリックします。
3. [データの選択]ページで、移行ファイルに含めるデータのカテゴリを選択してから**[次へ]**をクリックします。
4. [移行ファイル]ページで、ファイル名を入力するか、**[参照]**をクリックして場所を探し、**[次へ]**をクリックします。
5. パスワードの入力と確認を行い、**[次へ]**をクリックします。

   注記：　移行ファイルを復元するときに必要ですので、このパスワードは安全な場所に保管してください。

6. 選択したセキュリティ ログイン方法で認証します。
7. [移行ファイルを保存しました]ページで、**[完了]**をクリックします。

Privacy Manager の証明書および信頼済み連絡先の復元

別のコンピューター上での移行プロセスの一つとして、または同じコンピューター上で Privacy Manager の証明書と信頼済み連絡先を復元するには、以下の操作を行います。

1. Privacy Manager を開き、**[移行]**をクリックします。
2. **[復元]**をクリックします。
3. [移行ファイル]ページで、**[参照]**をクリックしてファイルを探し、**[次へ]**をクリックします。
4. バックアップ ファイル作成時に使用したパスワードを入力して、**[次へ]**をクリックします。
5. [移行ファイル]ページで、**[完了]**をクリックします。

Privacy Manager の集中管理

お使いの Privacy Manager のインストールは、管理者によってカスタマイズされ、集中化されたインストールの一部である可能性があります。以下の機能のうち 1 つ以上が、有効または無効にされている可能性があります。

- **証明書使用ポリシー**：証明書の使用は、Comodo によって発行される Privacy Manager 証明書に限定される場合があります。または、その他の証明機関によって発行されるデジタル証明書のみの使用が許可される場合があります。
- **暗号化ポリシー**：暗号化機能は、Microsoft Office または Microsoft Outlook、および Windows Live Messenger で、個別に有効または無効になっている可能性があります。

9 File Sanitizer for HP ProtectTools

File Sanitizer は、コンピューター上のフォルダーやファイル（個人情報やファイル、履歴データや Web 関連データ、その他のデータ コンポーネント）を安全にシュレッドしたり、ハードドライブを定期的に「ブリーチ（漂白）」したりすることができるツールです。

注記： このバージョンの File Sanitizer は、システム ハードドライブのみをサポートしています。

シュレッド

File Sanitizer を使用したフォルダーやファイルのシュレッドは、データの内容をわからなくするアルゴリズムが実行されて元のフォルダーやファイルを取り戻すことが事実上不可能になる点で、通常の Windows の削除（File Sanitizer ではシンプル削除とも言います）とは異なります。Windows のシンプル削除では、ファイル（またはフォルダー）がハードドライブ上にそのままの状態で残されるか、または電子情報の分析によって復元できる状態で残される可能性があります。

シュレッド プロファイル（[セキュリティ設定、高]、[セキュリティ設定、中]、または[セキュリティ設定、低]）を選択すると、あらかじめ定義されているフォルダーやファイルの一覧と消去方法がシュレッドのために自動で選択されます。また、シュレッド プロファイルをカスタマイズして、シュレッド サイクル数、シュレッド対象に含めるフォルダーやファイル、シュレッド前に確認するフォルダーやファイル、およびシュレッド対象から除外するフォルダーやファイルを指定することもできます。詳しくは、67 ページの 「シュレッド プロファイルの選択または作成」を参照してください。

自動シュレッドのスケジュールを設定することができます。また、必要に応じていつでもフォルダーやファイルを手動シュレッドすることもできます。詳しくは、66 ページの 「シュレッド スケジュールの設定」、71 ページの 「単一フォルダーやファイルの手動シュレッド」、または71 ページの「選択されているすべてのフォルダーやファイルの手動シュレッド」を参照してください。

注記： .dll ファイルは、ゴミ箱に移動されている場合にのみ、シュレッドされてシステムから削除されます。

空き領域ブリーチ

Windows でフォルダーやファイルを削除しても、その内容はハードドライブから完全に削除されません。Windows はフォルダーやファイルの参照情報のみを削除します。他のフォルダーやファイルによってハードドライブの同じ領域を新しい情報で上書きしないかぎり、フォルダーやファイルの内容はハードドライブに引き続き残ったままとなります。

空き領域ブリーチを実行すると、削除されたフォルダーやファイルに対してランダムなデータを安全に上書きできるため、削除されたフォルダーやファイルの元の内容をユーザーは参照できなくなります。

注記： 空き領域ブリーチは、Windows のゴミ箱を使用して削除したフォルダーやファイル、または手動で削除したフォルダーやファイルを対象とする機能です。空き領域ブリーチを実行しても、シュレッドされたフォルダーやファイルにセキュリティが追加されることはありません。

タスクバーの右端の通知領域にある**[HP ProtectTools]**アイコンを使用して、空き領域ブリーチの自動スケジュールを有効にするか、空き領域ブリーチを手動で実行することができます。詳しくは、67 ページの 「空き領域ブリーチのスケジュール設定」、または72 ページの 「空き領域ブリーチの手動実行」を参照してください。

セットアップ手順

File Sanitizer の起動

File Sanitizer を起動するには、以下の操作を行います。

1. **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャー）の順にクリックします。
2. **[File Sanitizer]**をクリックします。

または

▲ デスクトップにある**[File Sanitizer]**アイコンをダブルクリックします。

または

▲ タスクバーの右端の通知領域にある**[HP ProtectTools]**アイコンを右クリックしてから、**[File Sanitizer]**→**[File Sanitizer を開く]**の順にクリックします。

シュレッド スケジュールの設定

注記： あらかじめ定義されているシュレッド プロファイルの選択またはシュレッド プロファイルの作成については、67 ページの 「シュレッド プロファイルの選択または作成」を参照してください。

注記： フォルダーやファイルの手動シュレッドについては、71 ページの 「単一フォルダーやファイルの手動シュレッド」を参照してください。

1. File Sanitizer を起動して、**[シュレッド]**をクリックします。
2. シュレッド オプションを以下の中から選択します。
   - **[Windows のシャットダウン時]**：選択されているすべてのフォルダーやファイルを Windows のシャットダウン時にシュレッドするには、このオプションを選択します。

     注記： このオプションを選択すると、シャットダウン時にダイアログ ボックスが表示され、選択されているフォルダーやファイルのシュレッドを実行するか、シュレッド処理を中止するかを確認します。シュレッド処理に進む場合は**[はい]**、シュレッドを中止する場合は**[いいえ]**をクリックします。
   - **[Web ブラウザーの起動時]**：ブラウザーの URL 履歴など、選択されているすべての Windows 関連フォルダーやファイルを Web ブラウザーの起動時にシュレッドするには、このオプションを選択します。
   - **[Web ブラウザーの終了時]**：ブラウザーの URL 履歴など、選択されているすべての Windows 関連フォルダーやファイルを Web ブラウザーの終了時にシュレッドするには、このオプションを選択します。
   - **[キーの組み合わせ]**：キーの組み合わせでシュレッドを開始するには、このオプションを選択します。
   - **[スケジューラ]**：**[スケジューラの起動]**チェック ボックスにチェックを入れ、Windows のパスワードを入力してから、選択されているフォルダーやファイルをシュレッドする日付と時刻を入力します。

注記： .dll ファイルは、ゴミ箱に移動されている場合にのみ、シュレッドされてシステムから削除されます。

3. **[適用]→[OK]**の順にクリックします。

空き領域ブリーチのスケジュール設定

注記： 空き領域ブリーチは、Windows のゴミ箱を使用して削除したフォルダーやファイル、または手動で削除したフォルダーやファイルを対象とする機能です。空き領域ブリーチを実行しても、シュレッドされたフォルダーやファイルにセキュリティが追加されることはありません。

空き領域ブリーチのスケジュールを設定するには、以下の操作を行います。

1. File Sanitizer を起動して、**[空き領域ブリーチ]**をクリックします。
2. **[スケジューラの起動]**チェック ボックスにチェックを入れ、Windows のパスワードを入力してから、ハードドライブをブリーチする日付と時刻を入力します。
3. **[適用]→[OK]**の順にクリックします。

注記： 空き領域ブリーチ操作は、長い時間がかかる場合があります。空き領域ブリーチはバックグラウンドで実行されますが、プロセッサの使用量が大きくなるため、コンピューターの動作が遅くなる場合があります。

シュレッド プロファイルの選択または作成

あらかじめ定義されているプロファイルを選択するか、自分のプロファイルを作成して、消去方法を指定したりシュレッドするフォルダーやファイルを選択したりすることができます。

あらかじめ定義されているシュレッド プロファイルの選択

あらかじめ定義されているシュレッド プロファイル（[セキュリティ設定、高]、[セキュリティ設定、中]または[セキュリティ設定、低]）を選択すると、あらかじめ定義されている消去方法とフォルダーやファイルの一覧が自動的に選択されます。**[詳細を表示]**ボタンをクリックすると、シュレッド用に選択されているフォルダーやファイルのあらかじめ定義されている一覧が表示されます。

あらかじめ定義されているシュレッド プロファイルを選択するには、以下の操作を行います。

1. File Sanitizer を起動し、**[設定]**をクリックします。
2. あらかじめ定義されているシュレッド プロファイルをクリックします。
3. **[詳細を表示]**をクリックして、シュレッド用に選択されているフォルダーやファイルの一覧を表示します。
4. **[次のフォルダー/ファイルをシュレッドする]**で、シュレッド前に確認する各フォルダーやファイルの横のチェック ボックスにチェックを入れます。
5. **[適用]→[OK]**の順にクリックします。

シュレッド プロファイルのカスタマイズ

シュレッド プロファイルを作成するには、シュレッド サイクル数、シュレッド対象に含めるフォルダーやファイル、シュレッド前に確認するフォルダーやファイル、およびシュレッド対象から除外するフォルダーやファイルを指定します。

1. File Sanitizer を起動し、**[設定]→[高度なセキュリティ設定]→[詳細を表示]**の順にクリックします。
2. シュレッド サイクル数を指定します。

   注記： 各フォルダーやファイルに対して、指定した数のシュレッド サイクルが実行されます。たとえば、シュレッド サイクルで「3」を選択すると、データの内容をわからなくするアルゴリズムが 3 つの別々の時間に実行されます。高いセキュリティ設定でシュレッド サイクルを選択すると、シュレッドに非常に長い時間がかかる場合があります。ただし、指定するシュレッド サイクル数を大きくするほど、データを取得できる可能性は低くなります。

3. シュレッドするフォルダーやファイルを選択するには、以下の操作を行います。
   a. **[使用できるシュレッド オプション]**で、フォルダーやファイルをクリックしてから**[追加]**をクリックします。
   b. カスタム フォルダーやファイルを追加するには、**[カスタムオプションの追加]**をクリックし、ファイル名やフォルダーのパスを選択または入力します。**[開く]→[OK]**の順にクリックします。**[使用できるシュレッド オプション]**で、追加するフォルダーやファイルをクリックしてから**[追加]**をクリックします。

   注記： [使用できるシュレッド オプション]からフォルダーやファイルを削除するには、削除するフォルダーやファイルをクリックしてから**[削除]**をクリックします。

4. **[次のフォルダーやファイルをシュレッドする]**で、シュレッド前に確認するフォルダーやファイルの横のチェック ボックスにチェックを入れます。

   注記： シュレッド リストからフォルダーやファイルを削除するには、フォルダーやファイルをクリックしてから**[削除]**をクリックします。

5. 自動シュレッドからファイルやフォルダーを保護するには、**[次のフォルダー/ファイルをシュレッドしない]**で**[追加]**をクリックしてから、ファイル名やフォルダー名へのファイル パスを選択または入力します。**[開く]→[OK]**の順にクリックします。

   注記： 除外リストからフォルダーやファイルを削除するには、フォルダーやファイルをクリックしてから**[削除]**をクリックします。

6. シュレッド プロファイルの設定を完了したら、**[適用]→[OK]**の順にクリックします。

シンプル削除プロファイルのカスタマイズ

シンプル削除プロファイルは、シュレッドしないで標準的なフォルダーやファイルの削除を実行します。シンプル削除プロファイルをカスタマイズするには、シンプル削除対象に含めるフォルダーやファイル、シンプル削除の実行前に確認するフォルダーやファイル、およびシンプル削除対象から除外するフォルダーやファイルを指定します。

注記： シンプル削除オプションを使用する場合は、手動で削除したファイルやフォルダー、または Windwos のゴミ箱を使用して削除されたファイルやフォルダーに空き領域ブリーチを随時実行できます。

シンプル削除プロファイルをカスタマイズするには、以下の操作を行います。

1. File Sanitizer を起動し、**[設定]→[シンプル削除設定]→[詳細を表示]**の順にクリックします。
2. 削除するフォルダーやファイルを選択するには、以下の操作を行います。
   a. **[使用できる削除オプション]**で、フォルダーやファイルをクリックしてから**[追加]**をクリックします。
   b. カスタム フォルダー/ファイルを追加するには、**[カスタムオプションの追加]**をクリックし、ファイル名またはフォルダー名を入力して**[OK]**をクリックします。カスタム フォルダー/ファイルをクリックして、**[追加]**をクリックします。

注記： 使用できる削除オプションからフォルダーやファイルを削除するには、フォルダーやファイルをクリックしてから**[削除]**をクリックします。

3. **[次のフォルダー/ファイルを削除する]**で、削除前に確認する各フォルダーやファイルの横のチェック ボックスにチェックを入れます。

注記： 削除リストからフォルダーやファイルを削除するには、フォルダーやファイルをクリックしてから**[削除]**をクリックします。

4. **[次のフォルダー/ファイルを削除しない]**で、**[追加]**をクリックして、削除対象から除外するフォルダーやファイルを指定します。

注記： 除外リストからフォルダーやファイルを削除するには、フォルダーやファイルをクリックしてから**[削除]**をクリックします。

5. シンプル削除プロファイルの設定を完了したら、**[適用]→[OK]**の順にクリックします。

一般的なタスク

File Sanitizer を使用すると、以下のタスクを実行できます。

- キーの組み合わせでシュレッドを開始：この機能によって、（たとえば、ctrl ＋ alt ＋ delete などの）キーの組み合わせを作成してシュレッドを開始することができます。詳しくは、70 ページの 「キーの組み合わせによるシュレッドの開始」を参照してください。
- [File Sanitizer]アイコンでシュレッドを開始：これは、Windows のドラッグ アンド ドロップと同様の機能です。詳しくは、71 ページの 「[File Sanitizer]アイコンの使用」を参照してください。
- 特定のフォルダーやファイルまたは選択されているすべてのフォルダーやファイルを手動シュレッド：この機能によって、通常のシュレッド スケジュールの実行前に、手動でフォルダーやファイルをシュレッドすることができます。詳しくは、71 ページの 「単一フォルダーやファイルの手動シュレッド」または71 ページの 「選択されているすべてのフォルダーやファイルの手動シュレッド」を参照してください。
- 空き領域ブリーチを手動で実行：この機能によって、空き領域ブリーチを手動で実行することができます。詳しくは、72 ページの 「空き領域ブリーチの手動実行」を参照してください。
- シュレッド操作または空き領域ブリーチ操作を停止：この機能によって、シュレッド操作または空き領域ブリーチ操作を停止することができます。詳しくは、72 ページの 「シュレッド操作または空き領域ブリーチ操作の停止」を参照してください。
- ログ ファイルを表示：この機能によって、シュレッドまたは空き領域ブリーチのログ ファイルを表示することができます。ログ ファイルには、最後のシュレッド操作または空き領域操作で発生したエラーや障害が記録されます。詳しくは、72 ページの 「ログ ファイルの表示」を参照してください。

注記： シュレッド操作または空き領域ブリーチ操作は、非常に長い時間がかかる場合があります。シュレッドや空き領域ブリーチはバックグラウンドで実行されますが、プロセッサの使用量が大きくなるため、コンピューターの動作が遅くなる場合があります。

キーの組み合わせによるシュレッドの開始

キーの組み合わせを指定するには、以下の操作を行います。

1. File Sanitizer を起動して、**[シュレッド]**をクリックします。
2. **[キーの組み合わせ]**チェック ボックスにチェックを入れます。
3. 使用できるボックスに文字を 1 つ入力します。
4. **[CTRL]**ボックスまたは**[ALT]**ボックスのどちらかを選択してから**[SHIFT]**ボックスを選択します。

   たとえば、s キーと ctrl ＋ shift キーを使用して自動シュレッドを開始するには、ボックスに s と入力してから、**[CTRL]**オプションと**[SHIFT]**オプションにチェックを入れます。

   注記： 設定済みの他のキーの組み合わせとは異なるキーの組み合わせを選択してください。

キーの組み合わせでシュレッドを開始するには、以下の操作を行います。

1. shift キーと ctrl キーまたは alt キー（または指定した組み合わせのキー）を押しながら、選択した文字キーを押します。
2. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

[File Sanitizer]アイコンの使用

△ **注意：** シュレッドしたフォルダーやファイルは復元できません。手動でシュレッドするために選択するフォルダーやファイルについては、十分に検討してください。

1. シュレッドするドキュメントまたはフォルダーに移動します。
2. シュレッドするフォルダーやファイルをデスクトップの[File Sanitizer]アイコンにドラッグします。
3. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

単一フォルダーやファイルの手動シュレッド

△ **注意：** シュレッドしたフォルダーやファイルは復元できません。手動でシュレッドするために選択するフォルダーやファイルについては、十分に検討してください。

1. タスクバーの右端の通知領域にある**[HP ProtectTools]**アイコンを右クリックしてから、**[File Sanitizer]**→**[単一フォルダー/ファイルをシュレッド]**の順にクリックします。
2. [参照]ダイアログ ボックスが開いたら、シュレッドするフォルダーやファイルに移動してから**[OK]**をクリックします。

   注記： 選択できるフォルダーやファイルは、単一のファイルまたはフォルダーです。

3. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

または

1. デスクトップにある**[File Sanitizer]**アイコンを右クリックしてから、**[単一フォルダー/ファイルをシュレッド]**をクリックします。
2. [参照]ダイアログ ボックスが開いたら、シュレッドするフォルダーやファイルに移動してから**[OK]**をクリックします。
3. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

または

1. File Sanitizer を起動して、**[シュレッド]**をクリックします。
2. **[参照]**ボタンをクリックします。
3. [参照]ダイアログ ボックスが開いたら、シュレッドするフォルダーやファイルに移動してから**[OK]**をクリックします。
4. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

選択されているすべてのフォルダーやファイルの手動シュレッド

1. タスクバーの右端の通知領域にある**[HP ProtectTools]**アイコンを右クリックしてから、**[File Sanitizer]**→**[今すぐシュレッド]**の順にクリックします。
2. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

または

1. デスクトップにある**[File Sanitizer]**アイコンを右クリックしてから、**[今すぐシュレッド]**をクリックします。
2. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

または

1. File Sanitizer を起動して、**[シュレッド]**をクリックします。
2. **[今すぐシュレッド]**ボタンをクリックします。
3. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

空き領域ブリーチの手動実行

1. タスクバーの右端の通知領域にある**[HP ProtectTools]**アイコンを右クリックしてから、**[File Sanitizer]**→**[今すぐブリーチ]**の順にクリックします。
2. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

または

1. File Sanitizer を起動して、**[空き領域ブリーチ]**をクリックします。
2. **[今すぐブリーチ]**をクリックします。
3. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

シュレッド操作または空き領域ブリーチ操作の停止

シュレッド操作または空き領域ブリーチ操作の実行中、通知領域にある[HP ProtectTools セキュリティ マネージャー]アイコンの上にメッセージが表示されます。このメッセージには、シュレッド処理または空き領域ブリーチ処理の詳細（完了した割合）と、操作を停止するためのオプションが表示されます。

この操作を停止するには、以下の操作を行います。

▲ メッセージをクリックしてから**[停止]**ボタンをクリックすると、操作がキャンセルされます。

ログ ファイルの表示

シュレッド操作または空き領域ブリーチ操作を実行するたびに、エラーのログ ファイルまたは障害のログ ファイルが生成されます。これらのログ ファイルは、最新のシュレッド操作または空き領域ブリーチ操作に従って常に更新されます。

注記： 正常にシュレッドまたはブリーチされたファイルは、ログ ファイルには表示されません。

ログ ファイルには、シュレッド操作について作成されるファイルと空き領域ブリーチ操作について作成されるファイルがあります。これらのログ ファイルは、ハードドライブ上の以下の場所にあります。

- C:¥Program Files¥Hewlett-Packard¥File Sanitizer¥*[Username]*（ユーザー名）_ShredderLog.txt
- C:¥Program Files¥Hewlett-Packard¥File Sanitizer¥*[Username]*_DiskBleachLog.txt

10 Device Access Manager for HP ProtectTools（一部のモデルのみ）

Device Access Manager for HP ProtectTools を使用すると、Windows オペレーティング システムの管理者は、システム上のデバイスへのアクセスを制御し、不正なアクセスを防止することができます。

- アクセスを許可または拒否するデバイスを定義するためのデバイス プロファイルが、ユーザーごとに作成されます。
- また、ユーザーはグループに分けられます。あらかじめ定義されているデバイス管理者グループを使用することも、[コントロール パネル]の[管理ツール]にある[コンピュータの管理]オプションでグループを定義することもできます。
- グループ メンバーシップに基づいて、デバイス アクセスを許可または拒否できます。
- CD-ROM ドライブや DVD ドライブなどのデバイス クラスの場合は、読み取りアクセスおよび書き込みアクセスを個別に許可または拒否できます。

特定のユーザーに対して、デバイス アクセス制御ポリシーを読み取ったり変更したりするためのアクセス権を与えることもできます。

セットアップ手順

Device Access Manager を開く

Device Access Manager を開くには、以下の操作を行います。

1. **[スタート]→[すべてのプログラム]→[HP]→[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. 左側の枠内で、**[Device Access Manager]**（デバイス アクセス マネージャー）をクリックします。

デバイス アクセスの設定

Device Access Manager for HP ProtectTools には、以下の 3 つのビューがあります。

- [簡易構成]ビュー：デバイス管理者グループのメンバーに対して、デバイス クラスへのアクセスを許可または拒否するために使用します。
- [デバイス クラス構成]ビュー：特定のユーザーまたはグループに対して、特定の種類のデバイスまたは特定のデバイスへのアクセスを許可または拒否するために使用します。
- [ユーザー アクセス設定]ビュー：[簡易構成]および[デバイス クラス構成]の情報を表示または変更できるユーザーを指定するために使用します。

デバイス管理者グループ

Device Access Manager をインストールすると、デバイス管理者グループが作成されます。

デバイスへのアクセスという点で信頼できるユーザーとして分類されていないユーザーによるデバイス クラス セットへのアクセスを拒否することで、システム管理者は簡易的なデバイス アクセス制御ポリシーを設定できます。「デバイスに対して信頼できる」ユーザーと「デバイスに対して信頼できない」ユーザーを分けるには、「デバイスに対して信頼できる」すべてのユーザーをデバイス管理者のメンバーにすることをおすすめします。デバイス管理者グループのメンバーに対し、[簡易構成]または[デバイス クラス構成]ビューを通してデバイスへのアクセスを許可することによって、「デバイスに対して信頼できる」ユーザーに、指定されたデバイス クラス セットへのフル アクセスが確実に許可されます。

注記： ユーザーをデバイス管理者に追加しても、そのユーザーによるデバイスへのアクセスが自動的に許可されるわけではありません。しかし、[簡易構成]ビューを使用すれば、「デバイスに対して信頼できる」ユーザーに対し、必要なデバイス クラスセットへのアクセスを許可できます。

ユーザーをデバイス管理者に追加するには、以下の操作を行います。

- Windows 7、Windows Vista、または Windows XP Professional の場合は、標準の[ローカル ユーザーとグループ]MMC スナップインを使用します。
- Windows 7、Windows Vista、または Windows XP の各 Home Edition の場合は、権限のあるアカウントからコマンド プロンプト ウィンドウで以下のように入力します。

  c:¥> net localgroup "Device Administrators" ユーザー名 /ADD

簡易構成

管理者および承認されたユーザーは、[簡易構成]ビューを使用して、デバイス管理者以外のすべてのユーザーによる以下のデバイス クラスへのアクセスを変更できます。

注記： このビューを使用してデバイス アクセス情報を読み取るには、**[ユーザー アクセス設定]**ビューで、ユーザーまたはグループに対して「読み取り」アクセスを許可する必要があります。このビューを使用してデバイス アクセス情報を変更するには、**[ユーザー アクセス設定]**ビューで、ユーザーまたはグループに対して「変更」アクセスを許可する必要があります。

- すべてのリムーバブル メディア（フロッピーディスク、USB フラッシュ ドライブなど）
- すべての DVD/CD-ROM ドライブ
- すべてのシリアル コネクタおよびパラレル コネクタ
- すべての Bluetooth®デバイス
- すべての赤外線装置
- すべてのモデム デバイス
- すべての PCMCIA デバイス
- すべての 1394 デバイス

デバイス管理者以外のすべてのユーザーによるデバイス クラスへのアクセスを許可または拒否するには、以下の操作を行います。

1. **[HP ProtectTools 管理者コンソール]**の左側の枠内で、**[Device Access Manager]**→**[簡易構成]**の順にクリックします。
2. アクセスを拒否するには、右側の枠内で、デバイス クラスまたは特定のデバイスのチェック ボックスにチェックを入れます。アクセスを許可するには、デバイス クラスまたは特定のデバイスのチェックボックスのチェックを外します。

   チェック ボックスがグレーで表示されている場合は、アクセス方法に影響を与える値が[デバイス クラス構成]ビューで変更されています。この変更された値をリセットして簡易設定に戻すには、チェック ボックスのチェックを入れるかチェックを外し、**[はい]**をクリックして確認します。
3. **[保存]**アイコンをクリックします。

   注記： バックグラウンド サービスが実行されていない場合は、サービスを開始するかどうかを尋ねるダイアログ ボックスが表示されます。**[はい]**をクリックします。
4. **[OK]**をクリックします。

バックグラウンド サービスの開始

デバイス プロファイルを適用しようとすると、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）によって、[HP ProtectTools Device Locking/Auditing（HP ProtectTools デバイス ロック/検査）]バックグラウンド サービスを開始するかどうかを尋ねるダイアログ ボックスが表示されます。**[はい]**をクリックします。バックグラウンド サービスが開始され、以降はシステムが起動するたびにサービスが自動的に開始されるようになります。

注記： バックグラウンド サービスの開始を尋ねる画面が表示される前に、デバイス プロファイルを定義しておく必要があります。

管理者も、以下の操作を行ってこのサービスを開始または停止できます。

1. **[スタート]→[コントロール パネル]**の順にクリックします。
2. **[管理ツール]→[サービス]**の順にクリックします。
3. HP ProtectTools Device Locking/Auditing サービスを検索して設定します。

HP ProtectTools Device Locking/Auditing サービスを停止しても、デバイス ロックは停止されません。デバイス ロックは、次の 2 つのコンポーネントによって実行されています。

- HP ProtectTools Device Locking/Auditing サービス
- DAMDrv.sys ドライバー

サービスを開始するとこのデバイス ドライバーが開始されますが、サービスを停止してもこのドライバーは停止されません。

このバックグラウンド サービスが実行されているかどうかを確認するには、コマンド プロンプト ウィンドウを開いて「sc query flcdlock」と入力します。

このデバイス ドライバーが実行されているかどうかを確認するには、コマンド プロンプト ウィンドウを開いて「sc query damdrv」と入力します。

デバイス クラス構成

管理者および承認されたユーザーは、デバイス クラスまたは特定のデバイスへのアクセスを許可または拒否されているユーザーおよびグループを一覧から表示したり編集したりできます。

注記： このビューを使用してデバイス アクセス情報を読み取るには、**[ユーザー アクセス設定]**ビューで、ユーザーまたはグループに対して「読み取り」アクセスを許可する必要があります。このビューを使用してデバイス アクセス情報を変更するには、**[ユーザー アクセス設定]**ビューで、ユーザーまたはグループに対して「変更」アクセスを許可する必要があります。

[デバイス クラス構成]ビューには以下のセクションがあります。

- **[デバイス一覧]**：デバイス クラス、およびシステムにインストールされているか以前にインストールされていた可能性のあるデバイスをすべて表示します。
  - 保護は、通常はデバイス クラスに対して適用されます。ユーザーまたはグループを選択すると、そのデバイス クラスの任意のデバイスにアクセスできるようになります。
  - 特定のデバイスに対して保護を適用することもできます。
- **[ユーザー一覧]**：選択されたデバイス クラスまたは特定のデバイスへのアクセスを許可または拒否されているユーザーおよびグループをすべて表示します。
  - [ユーザー一覧]には、特定のユーザーまたはそのユーザーがメンバーとなっているグループを登録できます。
  - [ユーザー一覧]でユーザーまたはグループを利用できない場合は、設定が[デバイス一覧]のデバイス クラスまたは[クラス]フォルダーから継承されています。
  - DVD や CD-ROM など一部のデバイス クラスでは、読み取りおよび書き込み操作のためのアクセスを個別に許可または拒否することによって詳細な制御を設定できます。

    それ以外のデバイスおよびクラスでは、読み取りおよび書き込みアクセス権を継承できます。たとえば、読み取りアクセス権は上位のクラスから継承し、書き込みアクセス権はユーザーまたはグループごとに定義するといった設定が可能です。

注記： [読み取り]チェック ボックスのチェックが外れている場合、アクセス制御の登録内容はデバイスへの読み取りアクセスに影響を与えません。デバイスへの読み取りアクセスが許可されることも、拒否されることもありません。

例 1：ユーザーまたはグループがデバイスまたはデバイス クラスへの書き込みアクセスを拒否されている場合

このユーザー、このグループ、またはこのグループのメンバーには、デバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、書き込みアクセスまたは読み取りおよび書き込みアクセスを許可できます。

例 2：ユーザーまたはグループがデバイスまたはデバイス クラスへの書き込みアクセスを許可されている場合

このユーザー、このグループ、またはこのグループのメンバーには、同じデバイスまたはデバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、書き込みアクセスまたは読み取りおよび書き込みアクセスを拒否できます。

例 3：ユーザーまたはグループがデバイスまたはデバイス クラスへの読み取りアクセスを許可されている場合

このユーザー、このグループ、またはこのグループのメンバーには、同じデバイスまたはデバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、書き込みアクセスまたは読み取りおよび書き込みアクセスを許可できます。

例 4：ユーザーまたはグループがデバイスまたはデバイス クラスへの読み取りアクセスを拒否されている場合

このユーザー、このグループ、またはこのグループのメンバーには、デバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、読み取りアクセスまたは読み取りおよび書き込みアクセスを許可できます。

例 5：ユーザーまたはグループがデバイスまたはデバイス クラスへの読み取りおよび書き込みアクセスを許可されている場合

このユーザー、このグループ、またはこのグループのメンバーには、同じデバイスまたはデバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、書き込みアクセスまたは読み取りおよび書き込みアクセスを拒否できます。

例 6：ユーザーまたはグループがデバイスまたはデバイス クラスへの読み取りおよび書き込みアクセスを拒否されている場合

このユーザー、このグループ、またはこのグループのメンバーには、デバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、読み取りアクセスまたは読み取りおよび書き込みアクセスを許可できます。

ユーザーまたはグループのアクセス拒否

ユーザーまたはグループによるデバイスまたはデバイス クラスへのアクセスを拒否するには、以下の操作を行います。

1. **[HP ProtectTools 管理者コンソール]**の左側の枠内で、**[Device Access Manager]**→**[デバイス クラス構成]**の順にクリックします。
2. デバイスの一覧で、設定するデバイス クラスをクリックします。
   - デバイス クラス
   - すべてのデバイス
   - 個々のデバイス
3. **[ユーザー/グループ]**で、アクセスを拒否するユーザーまたはグループをクリックします。
4. ユーザーまたはグループの横にある**[拒否]**をクリックします。
5. **[保存]**アイコンをクリックします。

注記： 同じデバイス レベルでユーザーに対して拒否および許可を設定すると、アクセス許可よりもアクセス拒否が優先されます。

ユーザーまたはグループのアクセス許可

ユーザーまたはグループによるデバイスまたはデバイス クラスへのアクセスを許可するには、以下の操作を行います。

1. **[HP ProtectTools 管理者コンソール]**の左側の枠内で、**[Device Access Manager]**→**[デバイス クラス構成]**の順にクリックします。
2. デバイスの一覧で、以下のどれかをクリックします。
   - デバイス クラス
   - すべてのデバイス
   - 個々のデバイス
3. **[追加]**をクリックします。

   [ユーザーまたはグループの選択]ダイアログ ボックスが表示されます。
4. **[詳細]**をクリックし、**[今すぐ検索]**をクリックして、追加するユーザーまたはグループを検索します。
5. 使用可能なユーザーおよびグループの一覧に追加するユーザーまたはグループをクリックして**[OK]**をクリックします。
6. 再度**[OK]**をクリックします。
7. **[許可]**をクリックして、そのユーザーまたはグループによるアクセスを許可します。
8. **[保存]**アイコンをクリックします。

ユーザーまたはグループのアクセス削除

ユーザーまたはグループによるデバイスまたはデバイス クラスへのアクセスを削除するには、以下の操作を行います。

1. **[HP ProtectTools 管理者コンソール]**の左側の枠内で、**[Device Access Manager]**→**[デバイス クラス構成]**の順にクリックします。
2. デバイスの一覧で、設定するデバイス クラスをクリックします。
   - デバイス クラス
   - すべてのデバイス
   - 個々のデバイス
3. **[ユーザー/グループ]**で、削除するユーザーまたはグループをクリックし、**[削除]**をクリックします。
4. **[保存]**アイコンをクリックします。

グループの単一ユーザーによるデバイス クラスへのアクセス許可

単一のユーザーによるデバイス クラスへのアクセスを許可しながら、そのユーザーのグループのその他のメンバーによるアクセスを拒否するには、以下の操作を行います。

1. **[HP ProtectTools 管理者コンソール]**の左側の枠内で、**[Device Access Manager]**→**[デバイス クラス構成]**の順にクリックします。
2. デバイスの一覧で、設定するデバイス クラスをクリックします。
   - デバイス クラス
   - すべてのデバイス
   - 個々のデバイス
3. **[ユーザー/グループ]**で、アクセスを拒否するグループを選択し、**[拒否]**をクリックします。
4. 目的のクラスの下のフォルダーに移動して、特定のユーザーを追加します。
5. **[許可]**をクリックして、そのユーザーによるアクセスを許可します。
6. **[保存]**アイコンをクリックします。

グループの単一ユーザーによる特定のデバイスへのアクセス許可

管理者は、あるユーザーによる特定のデバイスへのアクセスを許可し、そのユーザーのグループのその他のメンバーによる、クラス内のすべてのデバイスへのアクセスは拒否するように設定できます。

1. **[HP ProtectTools 管理者コンソール]**の左側の枠内で、**[Device Access Manager]**→**[デバイス クラス構成]**の順にクリックします。
2. デバイスのリストで、設定するデバイス クラスをクリックして、その下のフォルダーに移動します。
3. **[追加]**をクリックします。**[ユーザーまたはグループの選択]**ダイアログ ボックスが表示されます。
4. **[詳細]**をクリックし、**[今すぐ検索]**をクリックして、クラス内のすべてのデバイスへのアクセスを拒否するユーザーのグループを検索します。

5. グループをクリックし、**[OK]**をクリックします。
6. ユーザーによるアクセスを許可する、デバイス クラスの下の特定のデバイスに移動します。
7. **[追加]**をクリックします。**[ユーザーまたはグループの選択]**ダイアログ ボックスが表示されます。
8. **[詳細]**をクリックし、**[今すぐ検索]**をクリックして、追加するユーザーまたはグループを検索します。
9. アクセスを許可するユーザーをクリックして**[OK]**をクリックします。
10. **[許可]**をクリックして、そのユーザーによるアクセスを許可します。
11. **[保存]**アイコンをクリックします。

構成のリセット

△ **注意：** 構成をリセットすると、それまでに実行されたデバイスの構成変更がすべて破棄され、すべての設定が工場出荷時の設定値に戻ります。

構成設定を工場出荷時の値に戻すには、以下の操作を行います。

1. **[HP ProtectTools 管理者コンソール]**の左側の枠内で、**[Device Access Manager]**→**[デバイス クラス構成]**の順にクリックします。
2. **[リセット]**ボタンをクリックします。
3. **[はい]**をクリックして確認します。
4. **[保存]**アイコンをクリックします。

高度なタスク

構成設定へのアクセスの制御

[ユーザー アクセス設定]ビューでは、管理者が、[簡易構成]ページおよび[デバイス クラス構成]ページの使用を許可するグループまたはユーザーを指定します。

注記： [ユーザー アクセス設定]ビューで設定を変更するユーザーまたはグループは、[フル ユーザー管理者権限]を持っている必要があります。

- [簡易構成]および[デバイス クラス構成]の情報を表示するユーザーまたはグループには、[ユーザー アクセス設定]ビューで[構成設定の表示（読み取り専用)]アクセスを許可する必要があります。
- [簡易構成]および[デバイス クラス構成]の情報を変更するユーザーまたはグループには、[ユーザー アクセス設定]ビューで[構成設定の変更]アクセスを許可する必要があります。

注記： Administrators グループのメンバーであっても、[簡易構成]および[デバイス クラス構成]の情報を表示するには「読み取り」アクセスを、[簡易構成]および[デバイス クラス構成]を使用してデータを変更するには「変更」アクセスを許可する必要があります。

注記： すべてのユーザーおよびグループのアクセス レベルを評価した後、特定のアクセス レベルに対して[許可]も[拒否]も選択されていないユーザーがある場合、ユーザーはそのレベルでのアクセスを拒否されます。

既存のグループまたはユーザーに対するアクセスの許可

既存のグループまたはユーザーに対して、構成設定を表示または変更するためのアクセス権を与えるには、以下の操作を行います。

1. **[HP ProtectTools 管理者コンソール]**の左側の枠内で、**[Device Access Manager]**→**[ユーザー アクセス設定]**の順にクリックします。
2. アクセスを許可するグループまたはユーザーをクリックします。
3. **[アクセス権]**で、選択されているグループまたはユーザーに与えるアクセス権の種類を以下から選んで、**[許可]**をクリックします。

   注記： アクセス権は累積的に与えられます。たとえば、[構成設定の変更]アクセス権が与えられたユーザーには、[構成設定の表示（読み取り専用)]アクセス権が自動的に与えられます。[フル ユーザー管理者権限]を与えられたユーザーには、[構成設定の変更]アクセス権および[構成設定の表示（読み取り専用)]アクセス権も与えられます。

   - フル ユーザー管理者権限
   - 構成設定の変更
   - 構成設定の表示（読み取り専用）
4. **[保存]**アイコンをクリックします。

既存のグループまたはユーザーに対するアクセスの拒否

既存のグループまたはユーザーに対して、構成設定を表示または変更するためのアクセス権を拒否するには、以下の操作を行います。

1. **[HP ProtectTools 管理者コンソール]**の左側の枠内で、**[Device Access Manager]**→**[ユーザーアクセス設定]**の順にクリックします。
2. アクセスを拒否するグループまたはユーザーをクリックします。
3. **[アクセス権]**で、選択されているグループまたはユーザーに対して拒否するアクセス権の種類を以下から選んで、**[拒否]**をクリックします。
   - フル ユーザー管理者権限
   - 構成設定の変更
   - 構成設定の表示（読み取り専用）
4. **[保存]**アイコンをクリックします。

新しいグループまたはユーザーの追加

新しいグループまたはユーザーに対して、構成設定を表示または変更するためのアクセス権を与えるには、以下の操作を行います。

1. **[HP ProtectTools 管理者コンソール]**の左側の枠内で、**[Device Access Manager]**→**[ユーザーアクセス設定]**の順にクリックします。
2. **[追加]**をクリックします。**[ユーザーまたはグループの選択]**ダイアログ ボックスが表示されます。
3. **[詳細]**をクリックし、**[今すぐ検索]**をクリックして、追加するユーザーまたはグループを検索します。
4. グループまたはユーザーをクリックして**[OK]**をクリックし、再度**[OK]**をクリックします。
5. **[許可]**をクリックして、そのユーザーによるアクセスを許可します。
6. **[保存]**アイコンをクリックします。

グループまたはユーザーのアクセス権の削除

グループまたはユーザーに対して、構成設定を表示または変更するためのアクセス権を削除するには、以下の操作を行います。

1. **[HP ProtectTools 管理者コンソール]**の左側の枠内で、**[Device Access Manager]**→**[ユーザーアクセス設定]**の順にクリックします。
2. グループまたはユーザーをクリックして、**[削除]**をクリックします。
3. **[保存]**アイコンをクリックします。

関連ドキュメント

Device Access Manager for HP ProtectTools は、HP ProtectTools Enterprise Device Access Manager と互換性があります。HP ProtectTools Enterprise Device Access Manager とともに使用した場合は、Device Access Manager for HP ProtectTools の機能への読み取り専用アクセスが許可されます。

Device Access Manager for HP ProtectTools については、http://www.hp.com/hps/security/products/（英語サイト）または、HP ProtectTools の紹介サイト、http://h50146.www5.hp.com/products/portables/protecttools/を参照してください。

11 LoJack Pro for HP ProtectTools

Absolute Software 社が提供する Computrace LoJack Pro（別売）は、コンピューターの紛失や盗難という年々増え続ける問題に対処します。

このソフトウェアを有効にすると、ハードドライブが再フォーマットまたは交換されてもコンピューター内でのアクティブな状態を維持する Computrace エージェントが有効になります。

LoJack Pro によって、コンピューターのリモートでの監視、管理、および追跡が可能になります。コンピューターを紛失したり盗難されたりした場合は、Absolute Software 社の復旧チームがその復旧を支援します。*

注記： *この機能は、地理的な位置に依存します。詳しくは、Absolute Software 社のサブスクリプション契約を参照してください。

12 トラブルシューティング

HP ProtectTools Security Manager

簡単な説明	詳細	解決方法
HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）のインストール後に取り付けたスマート カードおよび USB トークンを Security Manager で利用できない	スマート カードまたは USB トークンを HP ProtectTools Security Manager で使用するには、それらのサポート ソフトウェア（ドライバー、PKCS#11 プロバイダーなど）を HP ProtectTools Security Manager より先にインストールする必要があります HP ProtectTools Security Manager がすでにインストールされている場合は、スマート カードまたはトークンのサポート ソフトウェアをインストールした後、解決方法にある操作を行います	パスワード マネージャーにログオンします HP ProtectTools Security Manager で、**[パスワード マネージャー]**→**[証明情報]**→**[スマート カード]**の順にクリックします。 再起動を求めるメッセージが表示されたら、コンピューターを再起動します
一部のアプリケーションの Web ページでエラーが発生し、ユーザーがタスクを実行または完了できなくなる	シングルサインオンの機能無効化パターンによって、一部の Web ベースのアプリケーションが機能を停止し、エラーを報告します。たとえば、Internet Explorer では黄色い三角形の中に**[!]**が表示され、エラーの発生を通知します	HP ProtectTools Security Manager シングルサインオンは、すべてのソフトウェアの Web インターフェイスをサポートしているわけではありません。シングルサインオンのサポートをオフにすることによって、特定の Web ページに対するシングルサインオンのサポートを無効にしてください。HP ProtectTools Security Manager のヘルプ ファイルに含まれている、シングルサインオンに関する詳しいドキュメントを参照してください 特定のアプリケーションで特定のシングルサインオンを無効にできない場合は、HP のサポート窓口にお問い合わせください
ログオン プロセス中に、**[仮想トークンの参照]**のオプションが表示されない	セキュリティ上のリスクを軽減するために参照のオプションが削除されたため、パスワード マネージャーで、ユーザーは登録された仮想トークンの場所を移動できません	参照のオプションは、ユーザー以外の利用者がファイルを削除したり、ファイルの名前を変更したりして Windows を制御できてしまうため、削除されました
権限がある場合でも、ドメイン管理者が Windows パスワードを変更できない	この問題は、ドメイン管理者がドメインにログオンし、そのドメインとローカル コンピューター上に管理者の権限を持つアカウントを使用して、パスワード マネージャーにドメイン ID を登録した後に発生します。ドメイン管理者がパスワード マネージャーから Windows パスワードを変更しようとすると、[ユーザー アカウントの制限]というログオン エラーが表示されます	パスワード マネージャーでは、**[Windows パスワードの変更]**を使用してドメイン ユーザーのアカウント パスワードを変更することはできません。HP ProtectTools Security Manager では、ローカル コンピューターのアカウント パスワードのみ変更可能です。ドメイン ユーザーは、**[Windows セキュリティ]**の**[パスワードの変更]**オプションを使用して自分のパスワードを変更できますが、ドメイン ユーザーはローカル コンピューター上に物理アカウントを持っていないため、パスワード マネージャーはログオンに使用されたパスワードしか変更できません

簡単な説明	詳細	解決方法
パスワード マネージャーに、Corel WordPerfect 12 のパスワード GINA との非互換性の問題がある	ユーザーがパスワード マネージャーにログオンし、WordPerfect でドキュメントを作成して、パスワード保護を使用して保存した場合、パスワード マネージャーは、パスワード GINA を（手動または自動にかかわらず）検出または認識することができません	HP では、将来の製品の機能強化に活かせるように、回避策を調査中です
パスワード マネージャーによって画面上の**[接続]**ボタンが認識されない	シングルサインオンが再起動されたときに、リモート デスクトップ接続（RDP）のシングルサインオン証明情報が**[接続]**に設定されていると、**[接続]**の代わりに常に**[名前を付けて保存]**が入力されます	HP では、将来の製品の機能強化に活かせるように、回避策を調査中です
Windows XP Service Pack 1 を使用している場合のみ、スリープ モードからハイバネーションに移行した後、パスワード マネージャーにログオンできない	システムがハイバネーションやスリープ モードに移行すると、選択されているログオン証明情報の種類（パスワード、指紋、または Java Card）にかかわらず、管理者やユーザーはパスワード マネージャーにログオンできなくなり、Windows のログオン画面が表示されたままになります	Windows Update を使用して、Windows を Service Pack 2 にアップデートしてください。この問題の原因について詳しくは、http://www.microsoft.com/japan/にあるマイクロソフト サポート技術情報の文書番号 813301 を参照してください ユーザーがログオンするには、パスワード マネージャーを選択してログオンする必要があります。パスワード マネージャーにログオンすると、Windows にログオンして（Windows ログオン オプションの選択が必要になる場合があります）ログオン プロセスを完了するよう要求されます ユーザーが最初に Windows にログオンした場合は、手動でパスワード マネージャーにログオンする必要があります
セキュリティの**[ID の復元]**プロセスで、仮想トークンとの関連付けが失われる	ユーザーが ID を復元したとき、パスワード マネージャーで、ログオン画面での仮想トークンの場所との関連付けが失われる場合があります。パスワード マネージャーには仮想トークンが登録されているにもかかわらず、ユーザーは関連付けを復元するためにトークンを再登録する必要があります	現在の仕様です ID を保存しないでパスワード マネージャーをアンインストールすると、トークンのシステム（サーバー）の部分が破壊されるため、トークンのクライアントの部分が ID の復元によって復元されたとしても、そのトークンはログオンに使用できなくなります HP では、一時的ではない解決策を調査中です

Device Access Manager for HP ProtectTools

Device Access Manager 内ではユーザーがデバイスへのアクセスを拒否されたが、これらのデバイスにユーザーが引き続きアクセス可能である場合

- **説明**：ユーザーによるデバイスへのアクセスを拒否するために、Device Access Manager 内では簡易構成やデバイス クラス構成が使用されてきました。アクセスを拒否されたにもかかわらず、ユーザーは引き続きデバイスにアクセスできます。
- **解決方法**：
  - HP ProtectTools デバイス ロック サービスが開始していることを確認してください
  - 管理者権限のあるユーザーとしてログインし、**[コントロール パネル]**→**[システムとメンテナンス]**の順にクリックします。[管理ツール]ウィンドウで**[サービス]**をクリックし、HP ProtectTools Device Locking/Auditing サービスを見つけます。このサービスが開始されていて、スタートアップの種類が**[自動]**であることを確認してください。

ユーザーがデバイスへの予期しないアクセスを許可されたり、ユーザーがデバイスへのアクセスを予期せず拒否されたりする場合

- **説明**：Device Access Manager は、一部のデバイスへのアクセスを拒否し、その他のデバイスへのアクセスを許可するために使用されてきました。ユーザーがシステムを使用中に、Device Access Manager によって拒否されていると思っていたデバイスにアクセスできたり、Device Access Manager によって許可されていると思っていたデバイスへのアクセスを拒否されたりすることがあります。
- **解決方法**：
  - ユーザーのデバイス設定の調査には、Device Access Manager の[デバイス クラス構成]を使用してください。
  - **[Security Manager]**（セキュリティ マネージャー）→**[Device Access Manager]**→**[デバイス クラス構成]**の順にクリックします。[デバイス クラス]ツリーの各レベルを展開し、このユーザーに該当する設定を確認します。そのユーザーに対して設定されている[拒否]アクセス権、またはそのユーザーがメンバーになっている Windows グループ（たとえば、Users、Administrators など）があるかどうかを確認してください。

許可と拒否のどちらが優先されるか

- **説明**：デバイス クラス構成内では、以下の構成が設定されています。
  - [許可]アクセス権は、ある Windows グループ（たとえば、BUILTIN\Administrators）に許可されています。一方、[拒否]アクセス権は、デバイス クラス階層内の同じレベル（たとえば、DVD/CD-ROM ドライブ）にある別の Windows グループ（たとえば、BUILTIN\Users）に許可されています
  - あるユーザーがこの両方のグループのメンバー（たとえば管理者）である場合は、どちらが優先されますか
- **解決方法**：
  - このユーザーはデバイスへのアクセスを拒否されます。拒否は許可より優先されます。
  - アクセスは、Windows でデバイスに対する有効なアクセス権が決定される方法に従って拒否されます。あるグループが拒否され、別のグループが許可されていますが、ユーザーはこの両方のグループのメンバーです。アクセスの拒否はアクセスの許可より優先されるため、このユーザーは拒否されます。

- 回避策の 1 つは、DVD/CD-ROM ドライブのレベルにある Users グループを拒否し、DVD/CD-ROM ドライブより低いレベルにある Administrators グループを許可することです
- 別の回避策として、DVD/CD へのアクセスを許可するための専用の Windows グループ、および DVD/CD へのアクセスを拒否するための専用の Windows グループを、別々に作成する方法もあります。それから、該当するグループに特定のユーザーを追加します。

[簡易構成]ビューを使用してデバイス アクセス制御ポリシーを定義したが、管理者権限のあるユーザーがデバイスにアクセスできない場合

- **説明**：[簡易構成]では、Users および Guests のアクセスが拒否され、デバイス管理者によるアクセスが許可されます。
- **解決方法**：管理者権限のあるユーザーを Administrators グループに追加します。

その他

影響を受けるソフトウェアの簡単な説明	詳細	解決方法
セキュリティ マネージャー：以下の警告が表示される。**[HP ProtectTools セキュリティ マネージャーがインストールされるまで、セキュリティ アプリケーションをインストールできません。]**	Java Card Security や指紋認証などのセキュリティ アプリケーションはすべて、セキュリティ マネージャー インターフェイスの拡張可能なプラグインです。HP が承認しているセキュリティ プラグインをロードするには、先に HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）をインストールしておく必要があります	セキュリティ プラグインをインストールする前に、セキュリティ マネージャー ソフトウェアをインストールしておく必要があります
HP ProtectTools Security Manager：セキュリティ マネージャー インターフェイスを閉じたとき、エラーが返されることがある	すべてのプラグイン アプリケーションのロードが終了する前に、セキュリティ マネージャーを閉じようとして画面右上の閉じるボタンを使用すると、エラーが発生することがあります（12 回に 1 回ぐらいの割合）	これは、セキュリティ マネージャーを終了および再起動するときに、そのタイミングがプラグイン サービス ロード時間の影響を受けることに関連しています。PTHOST.exe は、他のアプリケーション（プラグイン）を収納するシェルであるため、プラグインのロード時間（サービス）の終了能力の影響を受けます。この問題の根本原因は、プラグインのロード終了に必要な時間が経過していないときにシェルが閉じられたことです セキュリティ マネージャーがサービス ロード メッセージ（[HP ProtectTools Security Manager]ウィンドウの一番上に表示される）をすべて出力し、左の列にすべてのプラグインが一覧表示されるまで待ちます。エラーを回避するため、プラグインをロードするときは時間を十分にとってください
HP ProtectTools：無制限のアクセスや制御されていない管理権限によってセキュリティ上のリスクが生じる	クライアント コンピューターへのアクセスが無制限の場合、以下のような多くのリスクが生じる可能性があります ● PSD の削除 ● ユーザー設定への悪意のある変更 ● セキュリティ ポリシーや機能の無効化	管理者は、エンド ユーザーの権限の制限や、ユーザー アクセスの制限に関して「ベスト プラクティス（成功事例）」に従うことをおすすめします 権限のないユーザーには管理者権限を付与しないでください

用語集

[安全に送信]ボタン：　Microsoft Outlook の電子メール メッセージのツールバーに表示されるソフトウェア ボタン。このボタンをクリックすると、Microsoft Outlook の電子メール メッセージに対する署名や暗号化ができます。

[署名と暗号化]ボタン：　Microsoft Office アプリケーションのツールバーに表示されるソフトウェア ボタン。このボタンをクリックすると、Microsoft Office ドキュメントに対する署名、暗号化、または暗号化の解除ができます。

ATM：　Automatic Technology Manager。ネットワーク管理者がシステムを BIOS レベルでリモート管理できます。

Drive Encryption のログオン画面：　Windows が起動する前に表示されるログオン画面。ユーザーは、Windows のユーザー名およびパスワード、または Java Card の PIN を入力する必要があります。ほとんどの場合、Drive Encryption のログオン画面で正しい情報を入力すれば、Windows のログオン画面で再度ログインすることなく、直接 Windows にアクセスできます。

Drive Encryption：　ハードドライブを暗号化して、適切な権限のないユーザーが情報を読み取れないようにすることによってデータを保護します。

DriveLock：　ハードドライブをユーザーにリンクして、コンピューターの起動時にユーザーに正しい DriveLock パスワードの入力を要求するセキュリティ機能。

HP SpareKey：　Drive Encryption キーのバックアップ コピー。

ID：　HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）内で、特定のユーザーのアカウントまたはプロファイルのように処理される、証明情報と設定の集合。

ID カード：　ユーザー名および選択された画像を使用してデスクトップを視覚的に識別するための、Windows サイドバーのガジェット。HP ProtectTools 管理者コンソールを開くには、ID カードをクリックします。

Java Card：　コンピューターに挿入するリムーバブル カード。ログオン用の識別情報が保存されています。Drive Encryption のログオン画面で Java Card を使用してログインするには、Java Card を挿入し、ユーザー名および Java Card の PIN を入力する必要があります。

Live Messenger History Viewer：　暗号化されたチャット履歴セッションの検索と表示ができる、[Privacy Manager Chat]のコンポーネント。

PSD：　Personal Secure Drive。機密情報を保護するための記憶領域を提供する機能。

Privacy Manager の証明書：　電子メール メッセージおよび Microsoft Office ドキュメントに対する署名や暗号化など、暗号の演算に使用するたびに認証が必要なデジタル証明書。

SATA device mode（SATA デバイス モード）：　コンピューターと大容量ストレージ デバイス（ハードドライブやオプティカル ドライブなど）の間のデータ転送モード。

TXT：　Trusted Execution Technology（トラステッド エグゼキューション テクノロジ）の略。

USB トークン： ユーザーに関する識別情報が格納されているセキュリティ デバイス。Java Card や指紋認証システムと同様に、所有者をコンピューターに対して認証するために使用されます。

Windows ユーザー アカウント： ネットワークまたは個別のコンピューターへのログオンを承認された個人のプロファイル。

Windows ログオンのセキュリティ： アクセスのために特定の証明情報を使用するよう求めることで、Windows アカウントを保護できます。

Windows 管理者： アクセス権を変更し、他のユーザーを管理するすべての権限を持つユーザー。

暗号化サービス プロバイダー（CSP）： 明確なインターフェイスを使用して特定の暗号化関数を実行するための暗号化アルゴリズムの提供者またはライブラリ。

暗号化の解除： 暗号化されたデータを平文に変換するための、暗号法で使用される手順。

暗号化ファイル システム（EFS）： 選択されたフォルダー内のすべてのファイルおよびサブフォルダーを暗号化するシステム。

暗号化： 権限のない受信者がデータを解読できないように平文を暗号文に変換するための、暗号法で使用されるアルゴリズムなどの手順。データの暗号化にはさまざまな種類があり、ネットワーク セキュリティの基礎として使用されます。一般的な暗号化には、データ暗号化規格（DES）や公開キー暗号があります。

暗号法： 特定の個人のみが解読できるように、データを暗号化および暗号化解除する手法。

管理者： 「Windows 管理者」**を参照してください。**

キーの組み合わせ： 特定のキーの組み合わせ。ctrl ＋ alt ＋ s キーなどを押すと、自動シュレッドが開始されます。

緊急リカバリ アーカイブ： 他のプラットフォームの所有者キーを使用して基本ユーザー キーを再暗号化できる、保護された記憶領域。

グループ： デバイス クラスまたは特定のデバイスに対して同じレベルのアクセス許可またはアクセス拒否が設定されているユーザーのグループ。

PKI： 証明情報および暗号化キーを作成、使用、および管理するためのインターフェイスを定義する、公開キー基盤の規格。

コンソール： このプログラムの機能および設定に対するアクセスや管理を行うことができる、中心となる場所。

シングルサインオン： 認証情報を格納し、パスワード認証が必要なインターネットおよび Windows アプリケーションに HP ProtectTools Security Manager を使用してアクセスできるようにする機能。

シンプル削除： Windows のフォルダーやファイルの参照情報の削除。空き領域ブリーチを実行しても、フォルダーやファイルの内容をわからなくするデータをフォルダーやファイルに上書きしないかぎり、そのフォルダーやファイルの内容はハードドライブ上に残ります。

手動シュレッド： 単一のフォルダーやファイルまたは選択されている複数のフォルダーやファイルに対して、自動シュレッド スケジュールを省略して実行されるシュレッド。

シュレッド: フォルダーやファイルに含まれるデータの内容をわからなくするアルゴリズムの実行。

シュレッド サイクル： 各フォルダーやファイルでシュレッド アルゴリズムを実行する回数。選択したシュレッド サイクルの回数が多いほど、コンピューターのセキュリティは高くなります。

シュレッド プロファイル： あらかじめ指定されている消去方法とフォルダーやファイルの一覧。

スマート カード： 所有者に関する識別情報が格納されている、サイズと形状がクレジット カードに似た小さなハードウェア。所有者をコンピューターに対して認証するために使用されます。

セキュリティ ログイン方法： コンピューターへのログインに使用される方法。

ダッシュボード： このプログラムの機能および設定に対するアクセスや管理を行うことができる、中心となる場所。

チャット履歴セッション： チャット セッションでの双方の会話の記録が含まれている、暗号化されたファイル。

デジタル署名： 資料の送信者を証明し、署名された後にファイルが変更されていないことを証明するファイルとともに送信されるデータ。

デジタル証明書： デジタル証明書の所有者の身元と、デジタル情報の署名に使用される電子キーのペアとを結びつけることによって、個人または企業の身元を証明する電子的な信用証明書。

デバイス アクセス制御ポリシー： ユーザーがアクセスを許可または拒否されているデバイスの一覧。

デバイス クラス： ドライブなど、特定の種類にあてはまるすべてのデバイス。

電源投入時認証： Java Card、セキュリティ チップ、パスワードなど、コンピューターの起動時に何らかの形式の認証を要求するセキュリティ機能。

ドメイン： ネットワークの一部であり、共通のディレクトリ データベースを共有するコンピューターの集合。ドメインには一意の名前が付けられ、各ドメインには一連の共通の規則および手順が設定されます。

トークン： 「セキュリティ ログオン方法」を参照してください。

認証機関： 公開キー基盤の運営に必要な証明書を発行するサービス。

証明情報： ユーザーが認証プロセスで特定のタスクに対する適格性を証明するための方法。

ネットワーク アカウント： ローカル コンピューター上、ワークグループ内、またはドメイン上の Windows ユーザーまたは管理者のアカウント。

バイオメトリック（生体認証）： 指紋などの身体的な特徴を使用してユーザーを識別する認証証明のカテゴリ。

バックアップ： バックアップ機能を使用して、重要なプログラム情報のコピーをそのプログラムの外部の場所に保存すること。バックアップした内容は、後日、同じコンピューターまたは別のコンピューターに情報を復元するために使用できます。

バックグラウンド サービス： デバイス アクセス制御ポリシーを適用するには、HP ProtectTools Device Locking/Auditing（HP ProtectTools デバイス ロック/検査）バックグラウンド サービスが実行されている必要があります。このサービスは、[コントロール パネル]の[管理ツール]オプションにあるサービス アプリケーションで確認できます。このサービスが実行されていない場合、HP ProtectTools Security Manager は、デバイス アクセス制御ポリシーが適用されているときにサービスを起動しようと試みます。

フォルダー/ファイル： 個人の情報やファイル、履歴や Web 関連のデータなどを含むデータ コンポーネントのことで、ハードドライブ上に存在します。

ユーザー： Drive Encryption に登録された人。管理者以外のユーザーは、Drive Encryption での権限が制限されています。管理者以外のユーザーが実行できる操作は、登録（管理者の許可がある場合）とログインのみです。

リブート： コンピューターを再起動するプロセス。

ログオン： Web サイトやその他のプログラムにログオンするために使用できるユーザー名とパスワード（またはその他の選択された情報）で構成される、HP ProtectTools Security Manager 内のオブジェクト。

移行：　Privacy Manager の証明書および信頼済み連絡先を管理、復元、および転送する作業。

仮想トークン：　Java Card やカード リーダーとよく似た働きをするセキュリティ機能。このトークンは、コンピューターのハードドライブ上か、Windows レジストリ内のどちらかに保存されます。仮想トークンでログオンすると、認証を完了するためにユーザー PIN の入力を要求されます。

空き領域ブリーチ：　削除されたフォルダーやファイルにランダムなデータを安全に上書きして、削除されたフォルダーやファイルの元の内容をわからなくすることです。

公開：　ユーザーが 1 つ以上のチャット履歴セッションの暗号化を解除して、Contact Screen Name を平文で表示し、セッションを表示できるようにする作業。

指紋：　指紋の画像をデジタルの形式で抽出したもの。実際の指紋の画像は、HP ProtectTools Security Manager には保存されません。

自動シュレッド：　ユーザーが File Sanitizer で設定したスケジュールに従って実行されるシュレッドのことです。

署名欄：　デジタル署名を表示するためのプレースホルダー。ドキュメントに署名すると、署名者の名前と確認方法が表示されます。署名日と署名者のタイトルも表示できます。

承認されたユーザー：　[簡易構成]ビューまたは[デバイス クラス構成]ビューで構成設定を表示または変更するためのアクセス権を、[ユーザー アクセス設定]ビューで与えられているユーザー。

信頼できる IM 通信：　信頼できる送信者から信頼済み連絡先に宛てて、信頼できるメッセージを送信する通信セッション。

信頼できるメッセージ：　信頼できる送信者から信頼済み連絡先に宛てて、信頼できるメッセージを送信する通信セッション。

信頼できる送信者：　署名および暗号化した電子メールや Microsoft Office ドキュメントを送信する信頼済み連絡先。

信頼済み連絡先の一覧：　信頼済み連絡先の一覧。

信頼済み連絡先の受信者：　信頼済み連絡先になるための招待を受け取った人物。

信頼済み連絡先への招待状：　信頼済み連絡先になることを依頼するために送信された電子メール。

信頼済み連絡先宛てに封印：　電子メールにデジタル署名を付加した上で暗号化し、選択したセキュリティ ログオン方法による認証の後に送信する作業。

信頼済み連絡先：　信頼済み連絡先への招待を承認した人物。

推奨する署名者：　ドキュメントに署名欄を追加するために Microsoft Word または Microsoft Excel ドキュメントの所有者が指名したユーザー。

認証：　ユーザーがタスクの実行（コンピューターへのアクセス、特定のプログラムの設定変更、セキュリティ保護されたデータの表示など）を承認されているかどうかを確認するプロセス。

廃止パスワード：　ユーザーがデジタル証明書を要求するときに作成されるパスワード。このパスワードは、ユーザーがデジタル証明書を廃止する場合に必要です。これによって、ユーザー自身のみが証明書を廃止できるようになります。

復元：　プログラム情報を、以前に保存されたバックアップ ファイルからこのプログラムにコピーするプロセス。

有効化：　Drive Encryption の機能にアクセスする前に完了する必要があるタスク。Drive Encryption は、HP ProtectTools セットアップ ウィザードを使用して有効にします。管理者のみが Drive Encryption を有効にするこ

とができます。有効化プロセスは、ソフトウェアの有効化、ドライブの暗号化、ユーザー アカウントの作成、およびリムーバブル ストレージ デバイス上の初期バックアップ暗号化キーの作成で構成されます。

索引